PENERAPAN *HYBRID CRYPTOSYSTEM* MENGGUNAKAN METODE *ELLIPTIC CURVE CRYPTOGRAPHY* DAN *ADVANCED ENCRYPTION STANDARD* PADA KOMUNIKASI JARAK JAUH *LORA*

SKRIPSI

MUHAMMAD FATTAH

191401049

PROGRAM STUDI S-1 ILMU KOMPUTER

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UNIVERSITAS SUMATERA UTARA

MEDAN

2023

PENERAPAN *HYBRID CRYPTOSYSTEM* MENGGUNAKAN METODE *ELLIPTIC CURVE CRYPTOGRAPHY* DAN *ADVANCED ENCRYPTION STANDARD* PADA KOMUNIKASI JARAK JAUH *LORA*

Diajukan untuk melengkapi tugas dan memenuhi syarat memperoleh ijazah Sarjana Ilmu Komputer

MUHAMMAD FATTAH

191401049

PROGRAM STUDI S-1 ILMU KOMPUTER

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UNIVERSITAS SUMATERA UTARA

MEDAN

2023

PERSETUJUAN

Judul	:	PENERAPAN *HYBRID CRYPTOSYSTEM* MENGGUNAKAN METODE *ELLIPTIC CURVE CRYPTOGRAPHY* DAN *ADVANCED ENCRYPTION STANDARD* PADA KOMUNIKASI JARAK JAUH *LORA*
Kategori	:	SKRIPSI
Nama	:	MUHAMMAD FATTAH
Nomor Induk Mahasiswa	:	191401049
Program Studi	:	SARJANA (S-1) ILMU KOMPUTER
Fakultas	:	ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

Komisi Pembimbing:

Pembimbing 2

Prof. Dr. Syahril Efendi S.Si., M.IT.

NIP. 196711101996021001

Pembimbing 1

Seniman S.Kom., M.Kom.

NIP. 198705252014041001

Diketahui/disetujui oleh

Program Studi S-1 Ilmu Komputer

Ketua,

Dr. Amalia, S.T., M.T.

NIP. 197812212014042001

UNIVERSITAS SUMATERA UTARA

PERNYATAAN

PENERAPAN *HYBRID CRYPTOSYSTEM* MENGGUNAKAN METODE *ELLIPTIC CURVE CRYPTOGRAPHY* DAN *ADVANCED ENCRYPTION STANDARD* PADA KOMUNIKASI JARAK JAUH *LORA*

SKRIPSI

Saya mengakui bahwa skripsi ini adalah hasil karya saya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing telah disebutkan sumbernya.

Medan, 06 Desember 2023

Muhammad Fattah
191401049

PENGHARGAAN

Segala puji dan syukur atas kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul "Penerapan *Hybrid Cryptosystem* Menggunakan Metode *Elliptic Curve Cryptography* Dan *Advanced Encryption Standard* Pada Komunikasi Jarak Jauh *LoRa*" sebagai syarat memperoleh gelar Sarjana Komputer pada Program Studi S-1 Ilmu Komputer, Fakultas Ilmu Komputer dan Teknologi Informasi Univeristas Sumatera Utara. Dengan segala kerendahan hati, penulis ingin menyampaikan rasa hormat dan terimakasih yang sebesar-besarnya kepada semua pihak yang telah membantu dalam penyelesaian skripsi ini. Penulis mengucapkan terimakasih kepada:

1. Bapak Dr. Muryanto Amin, S.Sos., M.Si selaku Rektor Universitas Sumatera Utara.
2. Ibu Dr. Maya Silvi Lydia, B.Sc., M.Sc. selaku Dekan Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara.
3. Bapak Dr. Mohammad Andri Budiman, ST, M.Comp, Sc, MEM, S.C.J.P. selaku Wakil Dekan 1 Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara.
4. Ibu Dr. Amalia ST., M.T. selaku Kepala Program Studi S-1 Ilmu Komputer Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara.
5. Bapak Seniman S.Kom., M.Kom. selaku Dosen Pembimbing I yang telah memberikan bimbingan, saran, dan kritik kepada penulis.
6. Bapak Prof. Dr. Syahril Efendi S.Si., M.IT. selaku Dosen Pembimbing II yang juga telah memberikan bimbingan dan arahan kepada penulis.
7. Bapak/Ibu Penguji I yang telah memberikan saran dan masukan dalam penyempurnaan skripsi ini.
8. Bapak/Ibu Penguji II yang telah memberikan saran dan masukan dalam penyempurnaan skripsi ini.
9. Seluruh dosen dan staf pegawai Program Studi S1 Ilmu Komputer Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara.

10. Kedua orangtua penulis tercinta, serta Adik yang telah memberikan banyak doa, dukungan serta motivasi kepada penulis agar selalu semangat dalam menyelesaikan skripsi.
11. Teman-teman seperjuangan sekaligus sahabat semasa kuliah yang telah banyak memberikan bantuan, dukungan, serta hiburan selama masa perkuliahan.
12. Dan semua pihak yang terlibat secara langsung maupun tidak langsung yang telah banyak membantu yang tidak dapat disebutkan satu per satu. Semoga segala kebaikan, dukungan serta motivasi yang telah diberikan kepada penulis mendapat berkah dari Allah SWT

Medan, 06 Desember 2023

Penulis,

Muhammad Fattah

ABSTRAK

Komunikasi Long Range (*LoRa*) adalah teknologi komunikasi nirkabel yang sangat relevan dalam konteks *Internet of Things (IoT)* karena memungkinkan pengiriman data jarak jauh dengan efisiensi energi tinggi dan biaya yang rendah. Namun, dalam kemajuan teknologi tesebut, muncul tantangan besar terkait keamanan data yang dikirim melalui jaringan *LoRa*. Keamanan data sangat penting, terutama ketika data yang dikirim berisi informasi yang penting atau sensitif. Komunikasi *LoRa* menggunakan frekuensi terbuka, yang menjadi sumber kerentanan yang signifikan terhadap penyadapan dan manipulasi data oleh pihak yang tidak berwenang. Untuk mengatasi masalah tersebut, penelitian ini menerapkan konsep *Hybrid Cryptosystem* yang menggabungkan dua metode kriptografi *Elliptic Curve Cryptography (ECC)* dan *Advanced Encryption Standard (AES)*. Metode *ECC* merupakan metode kriptografi asimetris yang efisien untuk pembuatan kunci enkripsi. Metode *AES* merupakan metode kriptografi simetris yang cepat dan efisien dalam enkripsi dan dekripsi data. Metode *AES* digunakan untuk mengamankan data yang dikirim melalui jaringan *LoRa*. Penggunaan *Hybrid Cryptosystem* dengan *ECC* dan *AES* diharapkan dapat meningkatkan keamanan data dalam komunikasi *LoRa*, menjaga privasi, mencegah manipulasi, dan mengurangi risiko kesalahan yang berdampak serius. Selain itu, penelitian ini akan memberikan panduan praktis bagi pengembang perangkat dan aplikasi *LoRa* dalam mengimplementasikan solusi keamanan yang kuat.

Kata kunci: Kriptografi, *Hybrid Cryptosystem*, *AES*, *ECC*, *LoRa*

ABSTRACT

Long Range Communication (*LoRa*) is a wireless communication technology that is very relevant in the context of the *Internet of Things (IoT)* because it allows sending data over long distances with high energy efficiency and low cost. However, in this technological advancement, big challenges have emerged regarding the security of data sent via the *LoRa* network. Data security is very important, especially when the data sent contains important or sensitive information. *LoRa* communications use open frequencies, which is a source of significant vulnerability to eavesdropping and data manipulation by unauthorized parties. To overcome this problem, this research applies the *Hybrid Cryptosystem* concept which combines two cryptographic methods *Elliptic Curve Cryptography (ECC)* and *Advanced Encryption Standard (AES)*. The *ECC* method is an efficient asymmetric cryptography method for generating encryption keys. The *AES* method is a symmetric cryptography method that is fast and efficient in data encryption and decryption. The *AES* method is used to secure data sent over the *LoRa* network. The use of a *Hybrid Cryptosystem* with *ECC* and *AES* is expected to increase data security in *LoRa* communications, maintain privacy, prevent manipulation, and reduce the risk of errors that have serious consequences. Additionally, this research will provide practical guidance for *LoRa* device and application developers in implementing robust security solutions.

Keyword: Cryptography, *Hybrid Cryptosystem*, *AES*, *ECC*, *LoRa*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Komunikasi Long Range (*LoRa*) adalah teknologi komunikasi nirkabel yang banyak digunakan untuk berbagai hal dalam komunikasi pengiriman data. *LoRa* memungkinkan pengiriman data jarak jauh dengan efisiensi energi yang tinggi dan biaya yang rendah. Teknologi ini sangat relevan dalam konteks *Internet of Things (IoT)*, di mana perangkat-perangkat kecil dapat berkomunikasi secara nirkabel dengan pusat pengendalian. Namun, dalam kemajuan ini, timbul tantangan besar terkait dengan keamanan data yang dikirim melalui jaringan *LoRa*.

Keamanan data adalah salah satu aspek terpenting dalam komunikasi *LoRa*, terutama ketika data yang dikirimkan berisi informasi yang penting atau sensitif. Dalam penggunaan *IoT*, data yang dikirim melalui jaringan *LoRa* sering kali berhubungan dengan kesehatan, lingkungan, atau keamanan. Keamanan data yang buruk dapat mengakibatkan pelanggaran privasi, manipulasi data, atau bahkan potensi risiko keselamatan.

Salah satu ciri khas dari komunikasi *LoRa* adalah penggunaan frekuensi terbuka. Hal ini memungkinkan akses yang mudah oleh pihak yang tidak berwenang ke data yang dikirim melalui jaringan *LoRa*. Penggunaan frekuensi terbuka menjadi sumber kerentanan yang signifikan dalam konteks keamanan data pada komunikasi *LoRa*, karena data yang tidak dienkripsi dapat dengan mudah disadap dan dimanipulasi oleh pihak yang tidak berwenang.

Dalam upaya meningkatkan keamanan komunikasi *LoRa*, konsep *Hybrid Cryptosystem* dapat diterapkan sebagai pengamanan pengiriman data pada komunikasi *LoRa* sehingga mengurangi risiko penyadapan dan manipulasi data, sehingga menjaga integritas dan kerahasiaan informasi yang dikirimkan melalui komunikasi *LoRa*. *Hybrid Cryptosystem* menggabungkan dua atau lebih metode kriptografi untuk menciptakan tingkat keamanan yang lebih tinggi. Dalam hal ini, dua metode kriptografi yang digunakan adalah *Elliptic Curve Cryptography (ECC)* dan *Advanced Encryption*

Standard (AES). ECC adalah metode kriptografi asimetris yang memanfaatkan kurva eliptik dalam pembuatan kunci, sedangkan *AES* adalah algoritma enkripsi simetris yang efisien.

Elliptic Curve Cryptography (ECC) adalah metode kriptografi yang mengandalkan sifat matematis dari kurva eliptik untuk menghasilkan kunci enkripsi yang kuat. *ECC* telah terbukti lebih efisien dalam penggunaan sumber daya jika dibandingkan dengan metode kriptografi lainnya. Keunggulan ini membuat *ECC* sangat relevan dalam perangkat *IoT* yang memiliki keterbatasan daya dan sumber daya. *ECC* juga memiliki tingkat keamanan yang tinggi, sehingga cocok untuk melindungi data yang dikirim melalui jaringan *LoRa*.

Advanced Encryption Standard (AES) adalah algoritma enkripsi simetris yang telah diterima secara luas sebagai standar keamanan dalam berbagai aplikasi. *AES* menawarkan tingkat keamanan yang tinggi dan efisiensi yang baik dalam mengamankan data. Dalam konteks *Hybrid Cryptosystem*, *AES* digunakan untuk mengenkripsi dan mendekripsi data yang dikirim melalui jaringan *LoRa*. Keunggulan *AES* adalah kemampuannya untuk mengamankan data dengan cepat dan efisien, menjadikannya pilihan yang ideal dalam mengatasi tantangan keamanan dalam komunikasi *LoRa*.

Penggunaan *Hybrid Cryptosystem* dengan *ECC* dan *AES* dapat meningkatkan keamanan data dalam komunikasi *LoRa*, menjaga privasi, mencegah manipulasi, dan mengurangi risiko kesalahan yang dapat berdampak serius. Selain itu, penelitian ini akan memberikan panduan praktis bagi pengembang perangkat dan aplikasi *LoRa* dalam mengimplementasikan solusi keamanan yang kuat.

1.2 Rumusan Masalah

Frekuensi terbuka yang digunakan pada komunikasi *LoRa* menjadi sumber kerentanan dalam konteks keamanan pengiriman data, karena data yang tidak dienkripsi dapat dengan mudah disadap dan dimanipulasi oleh pihak yang tidak berwenang. Untuk itu dibutuhkan konsep *Hybrid Cryptosytem* untuk mengamankan data yang akan dikirim melalui komunikasi *LoRa*. Dalam hal ini, dua metode

kriptografi yang digabungkan pada konsep *Hybrid Cryptosystem* ini adalah *Elliptic Curve Cryptography (ECC)* dan *Advanced Encryption Standard (AES)*, sehingga dapat meningkatkan keamanan data dalam komunikasi *LoRa*, menjaga privasi, mencegah manipulasi, dan mengurangi risiko kesalahan.

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

1) Menggunakan modul sensor DHT11, BMP180, AJ-SR04M dan TS-300B sebagai inputan.
2) Menggunakan *LoRa* pada rentang frekuensi 800 MHz – 950MHz
3) Output ditampilkan pada *console* atau serial monitor berupa hasil dekripsi ciphertext.
4) Metode yang digunakan adalah *Elliptic Curve Cryptography (ECC)* dan *Advanced Encryption Standard (AES).*
5) Asumsi bahwa data yang dibaca oleh sensor DHT11, BMP180, AJ-SR04M dan TS-300B merupakan data yang penting dan sensitif.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengimplementasikan konsep *Hybrid Cryptosystem* menggunakan metode *Elliptic Curve Cryptography* dan *Advanced Encryption Standard* pada komunikasi jarak jauh *LoRa* sebagai solusi untuk meningkatkan keamanan data yang dikirim menggunakan komunikasi jarak jauh *LoRa*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1) Peningkatan Keamanan Komunikasi Jarak Jauh

   Penelitian ini akan memberikan manfaat langsung dalam meningkatkan keamanan berbagai komunikasi jarak jauh.

2) Efisiensi dan Kinerja yang Optimal

   Hybrid Cryptosystem yang dihasilkan dari penelitian ini diharapkan dapat memadukan keunggulan *ECC* dalam efisiensi penggunaan sumber daya dengan

kecepatan *AES* dalam proses enkripsi dan dekripsi data. Ini akan menghasilkan komunikasi jarak jauh yang lebih efisien tanpa mengorbankan tingkat keamanan.

3) Pengembangan Solusi Keamanan *IoT*

Penelitian ini dapat memberikan pandangan berharga untuk pengembangan solusi keamanan yang lebih kuat dalam konteks *Internet of Things (IoT)*. Hal ini akan bermanfaat bagi berbagai aplikasi *IoT*, termasuk smart city, pemantauan lingkungan, manajemen energi, dan banyak lagi, dengan memberikan tingkat kepercayaan yang lebih tinggi dalam pengiriman data.

4) Peningkatan Kesadaran Keamanan

Dengan mengembangkan solusi keamanan yang efektif, penelitian ini juga berpotensi meningkatkan kesadaran pentingnya keamanan dalam komunikasi jarak jauh, terutama dalam aplikasi kritis seperti sistem kesehatan jarak jauh dan keamanan smart city. Hal ini dapat membantu masyarakat lebih sadar tentang risiko dan langkah-langkah yang diperlukan untuk melindungi data mereka.

1.6 Metodologi Penelitian

Penelitian ini menerapkan beberapa metode penelitian sebagai berikut:

1) Studi Kasus

Dalam tahap ini penulis akan melakukan pengumpulan referensi yang dibutuhkan terkait dengan metode *ECC* dan metode *AES*. Referensi yang diambil dalam bentuk jurnal, artikel, makalah skripsi dan e-book.

2) Analisis dan Perancangan

Berdasarkan ruang lingkup penelitian, penulis akan melakukan analisa terhadap hal-hal yang dibutuhkan dalam penelitian dan membuat rancangan sistem.

3) Implementasi

Pada tahap ini, akan dilakukan proses implementasi metode *ECC* dan metode *AES* ke dalam bahasa pemrograman python.

4) Pengujian

Pada tahap ini, Di tahap pengujian akan dilakukan uji coba apakah keamanan data menggunakan implementasi kriptografi *ECC* dan *AES* sudah berjalan sesuai dengan kebutuhan.

5) Dokumentasi

Pada tahap ini, akan dilakukan proses dokumentasi mulai dari tahap analisa hingga tahap pengujian yang dibentuk dalam laporan penelitian (skripsi).

1.7 Sistematika Penulisan

Sistematika dalam penelitian disusun dalam format skripsi dan terbagi ke dalam beberapa bagian berikut:

BAB 1 PENDAHULUAN

Rangkuman mengenai latar belakang penelitian melibatkan rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Berisi penjelasan mengenai penjelasan teori tentang kriptografi, Algoritma simetris dan asimetris, *Hybrid Cryptosystem*, dasar matematika kriptografi metode *ECC*, metode *AES.*

BAB 3 ANALISIS DAN PERANCANGAN

Membahas analisis dan perancangan terkait dengan masalah penelitian. Ini mencakup analisis kebutuhan yang diperlukan dalam pengembangan sistem serta proses perancangan sistem yang akan dibangun.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Membahas penerapan metode *ECC*, dan metode *AES* pada protocol komunikasi *LoRa* dan pembahasan mengenai hasil pengujian sistem yang telah dibangun serta analisis dari hasil-hasil tersebut.

BAB 5 KESIMPULAN DAN SARAN

Kesimpulan dari hasil penelitian yang telah dilakukan dan saran yang diharapkan dapat berguna untuk pengembangan selanjutnya.

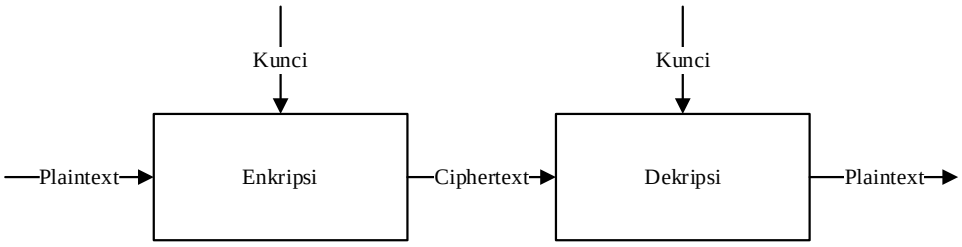
BAB 2
TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi dapat didefinisikan sebagai seni maupun ilmu yang menghasilkan pesan yang rahasia. Sebuah pesan asli yang disebut sebagai plaintext disandikan menjadi pesan yang tersandi yang disebut sebagai ciphertext melalui proses enkripsi dan ciphertext dipulihkan menjadi plaintext kembali melalui proses dekripsi.

Dalam konteks ini, kriptografi digunakan untuk menerapkan prinsip dan teknik tertentu guna menjaga pesan agar tidak dapat diakses oleh pihak yang tidak berwenang. Terdapat tiga fungsi dasar dalam kriptografi, yaitu:

1) Enkripsi merupakan sebuah proses di mana pesan aslinya, yang disebut sebagai plaintext, diubah menjadi kode yang tidak dapat dimengerti yang disebut ciphertext. Untuk menjalankan transformasi dari plaintext menjadi kode ini, diperlukan penerapan algoritma kriptografi yang memiliki kapabilitas untuk mengkodekan data tersebut.
2) Dekripsi, sebagai kebalikan dari enkripsi, adalah proses di mana pesan yang sebelumnya diubah menjadi ciphertext melalui enkripsi akan dikembalikan ke bentuk aslinya (plaintext).
3) Kunci, digunakan untuk mengoperasikan fungsi enkripsi dan dekripsi. Kunci ini terbagi menjadi dua jenis, yaitu kunci publik dan kunci pribadi.



Gambar 2.1 Proses Enkripsi Dan Dekripsi

2.2 Hybrid Cryptosystem

Hybrid Cryptosystem adalah pendekatan dalam kriptografi yang menggabungkan dua jenis kriptografi, yaitu kriptografi simetris dan kriptografi asimetris, untuk

menghasilkan tingkat keamanan yang tinggi dalam melindungi data. Pendekatan ini digunakan secara luas dalam berbagai aplikasi, terutama ketika perlu memastikan keamanan data selama pengiriman dan penyimpanan. Dalam *Hybrid Cryptosystem*, kunci enkripsi simetris yang kuat digunakan untuk mengenkripsi data yang sebenarnya. Kunci simetris adalah kunci yang sama digunakan untuk mengenkripsi dan mendekripsi data. Kunci ini biasanya lebih efisien dan lebih cepat dalam mengenkripsi data dibandingkan dengan kunci asimetris, yang membutuhkan lebih banyak daya komputasi.

Namun, satu tantangan dengan kunci simetris adalah bagaimana menyampaikan kunci tersebut kepada penerima dengan aman. Inilah di mana kriptografi asimetris masuk. Kunci publik dan kunci pribadi digunakan dalam kriptografi asimetris. Kunci publik digunakan untuk mengenkripsi data, sedangkan hanya kunci pribadi yang dapat mendekripsi data tersebut. Dalam *Hybrid Cryptosystem*, pengirim pertama-tama menghasilkan kunci simetris yang acak dan menggunakannya untuk mengenkripsi data yang akan dikirim. Kemudian, pengirim mengenkripsi kunci simetris ini menggunakan kunci publik penerima. Data yang dienkripsi dan kunci simetris yang juga telah dienkripsi dikirimkan ke penerima.

Ketika penerima menerima data yang telah dienkripsi, ia menggunakan kunci pribadi yang hanya dimilikinya untuk mendekripsi kunci simetris terlebih dahulu. Setelah itu, kunci simetris ini digunakan untuk mendekripsi data yang sebenarnya. Pendekatan ini mengatasi masalah distribusi kunci simetris dengan cara yang aman, karena kunci simetris yang dienkripsi dengan kunci publik hanya dapat didekripsi oleh penerima yang memiliki kunci pribadi yang sesuai. *Hybrid Cryptosystem* adalah pendekatan yang efektif dalam menggabungkan kecepatan dan efisiensi kriptografi simetris dengan keamanan kriptografi asimetris. Hal ini digunakan dalam banyak aplikasi yang memerlukan tingkat keamanan tinggi, seperti komunikasi aman melalui internet, pembayaran elektronik, dan perlindungan data pribadi. Dengan menggabungkan kelebihan keduanya, *Hybrid Cryptosystem* membantu memastikan bahwa data tetap aman dan rahasia saat berpindah tangan melalui jaringan yang tidak aman.

2.3 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) adalah metode kriptografi yang memanfaatkan kurva eliptik dalam matematika untuk melindungi data dan komunikasi dari akses yang tidak sah. Dalam *ECC*, keamanan berdasarkan sifat matematis dari kurva eliptik yang telah didefinisikan sebelumnya. Kurva eliptik ini adalah himpunan titik-titik yang mematuhi persamaan matematika tertentu. Salah satu karakteristik utama *ECC* adalah penggunaan pasangan kunci, yaitu kunci publik dan kunci pribadi. Kunci publik digunakan untuk mengenkripsi data, sedangkan kunci pribadi digunakan untuk mendekripsi data yang telah dienkripsi. Penggunaan pasangan kunci ini membuat *ECC* menjadi metode kriptografi asimetris, di mana kunci enkripsi berbeda dengan kunci dekripsi.

ECC memiliki beberapa keunggulan yang membuatnya menonjol dalam dunia kriptografi. Salah satunya adalah efisiensi penggunaan sumber daya. Karena *ECC* memerlukan panjang kunci yang relatif lebih pendek dibandingkan dengan metode kriptografi asimetris tradisional seperti RSA, hal ini menghasilkan kebutuhan daya komputasi dan bandwidth yang lebih rendah. Karena itu, *ECC* sangat cocok untuk perangkat dengan sumber daya terbatas, seperti perangkat *IoT*. Selain itu, *ECC* telah banyak digunakan dalam berbagai aplikasi, termasuk komunikasi nirkabel, teknologi sertifikat digital, tanda tangan digital, dan perlindungan data sensitif. Metode ini juga memiliki peran penting dalam keamanan sistem informasi dan perlindungan privasi.

Tabel 2.1 Perbandingan Panjang Kunci Kriptografi Simetris dan Asimetris

Panjang Kunci	Algoritma Simetris	FFC (DSA, DH, MQV)	IFC* (RSA)	ECC* (ECDSA, EdDSA, DH, MQV)
<= 80	2TDEA	L = 1024 N = 160	k = 10241	$f = 160 - 223$
112	3TDEA[68]	L = 2048 N = 224	k = 2048	$f = 224 - 255$
128	AES-128	L = 3072 N = 256	k = 3072	$f = 256 - 383$
192	AES-192	L = 7680 N = 384	k = 7680	$f = 384 - 511$
256	AES-256	L = 15360 N = 512	k = 15360	$f = 512 +$

Keamanan *ECC* bergantung pada panjang kunci yang digunakan. Semakin panjang kunci, semakin sulit bagi penyerang untuk memecah kunci dengan serangan brute force atau serangan lainnya. Oleh karena itu, pemilihan panjang kunci yang tepat adalah faktor kritis dalam implementasi *ECC* dengan tingkat keamanan yang memadai. Dalam pengembangan *ECC*, riset terus berlanjut untuk meningkatkan keamanan dan efisiensi metode ini, serta mengatasi tantangan keamanan yang mungkin muncul di masa mendatang, seperti serangan kuantum. *ECC* telah membuktikan diri sebagai metode kriptografi yang kuat dan efisien dalam era digital saat ini.

2.3.1 Elliptic Curve Diffie Hellman (ECDH)

Elliptic Curve Diffie-Hellman *(ECDH)* adalah sebuah protokol kriptografi yang menjadi bagian penting dalam menjaga keamanan komunikasi dan pertukaran kunci rahasia di dunia digital. Protokol ini didasarkan pada konsep kurva eliptik dalam matematika kriptografi, yang menghadirkan keamanan yang kuat dengan ukuran kunci yang relatif kecil. Dalam penjelasan berikut, kita akan membahas lebih lanjut mengenai *ECDH*, bagaimana itu berfungsi, serta mengapa itu penting dalam keamanan digital.

Pada dasarnya, *ECDH* dirancang untuk mengatasi dua tantangan utama dalam kriptografi modern: pertukaran kunci aman dan penggunaan sumber daya yang efisien. Pertukaran kunci adalah langkah awal dalam menjaga keamanan komunikasi. Dalam konteks ini, kunci mengacu pada serangkaian angka atau karakter yang digunakan untuk mengenkripsi dan mendekripsi pesan. Kunci rahasia yang kuat sangat penting, karena jika jatuh ke tangan yang salah, pesan-pesan tersebut dapat dengan mudah dipecahkan. *ECDH* mengatasi masalah ini dengan menghasilkan kunci rahasia bersama yang hanya dikenal oleh pihak yang sah.

ECDH bekerja dengan menghasilkan pasangan kunci, yaitu kunci publik dan kunci pribadi, yang terkait dengan kurva eliptik tertentu. Kunci publik dapat dengan aman dibagikan ke siapa pun tanpa membahayakan keamanan, sementara kunci pribadi harus tetap rahasia. Ketika dua pihak ingin berkomunikasi, mereka bertukar kunci publik mereka. Dengan menggunakan kunci publik yang diterima, setiap pihak dapat menghasilkan kunci rahasia bersama yang hanya dapat dihitung oleh mereka

berdasarkan kunci pribadi mereka. Kunci rahasia bersama ini kemudian digunakan untuk mengenkripsi dan mendekripsi pesan selama komunikasi.

Salah satu keuntungan utama *ECDH* adalah ukuran kunci yang relatif kecil. Ini membuatnya sangat efisien dalam penggunaan sumber daya, memungkinkan komunikasi yang cepat dan aman. Dalam perbandingan dengan metode tradisional, seperti Diffie-Hellman (tanpa kurva eliptik), *ECDH* membutuhkan lebih sedikit perhitungan dan ruang penyimpanan. Itulah sebabnya *ECDH* sangat populer dalam berbagai aplikasi, termasuk di perbankan online, pesan teks terenkripsi, dan keamanan data di *Internet of Things (IoT)*.

Selain itu, *ECDH* memiliki tingkat keamanan yang tinggi. Kurva eliptik yang digunakan dalam protokol ini menawarkan perlindungan yang kuat terhadap serangan kriptografis yang umum, seperti serangan brute-force. Ini menjadikan *ECDH* pilihan yang kuat untuk berbagai aplikasi keamanan. Bahkan dengan ukuran kunci yang relatif kecil, proses perhitungan kunci rahasia bersama yang dilakukan dalam *ECDH* sangat sulit untuk dipecahkan tanpa pengetahuan kunci pribadi yang sesuai.

Penting untuk dicatat bahwa *ECDH* hanya bertanggung jawab atas pertukaran kunci rahasia. Ini adalah langkah penting dalam menjaga kerahasiaan pesan, tetapi tidak mengenkripsi pesan itu sendiri. Setelah kunci rahasia bersama telah dibentuk, kunci ini dapat digunakan untuk mengenkripsi dan mendekripsi pesan melalui algoritma kriptografi yang sesuai, seperti *Advanced Encryption Standard (AES)*.

Dalam dunia digital yang penuh tantangan keamanan, *ECDH* telah menjadi salah satu alat kunci dalam menjaga kerahasiaan dan integritas informasi. Protokol ini mengatasi masalah pertukaran kunci dan penggunaan sumber daya yang efisien, menjadikannya pilihan yang sangat relevan untuk berbagai aplikasi, dari komunikasi aman hingga perlindungan data pribadi. Dengan ukuran kunci yang relatif kecil dan tingkat keamanan yang tinggi, *ECDH* membantu melindungi informasi dan komunikasi di dunia digital yang terus berkembang.

2.3.2 Kurva Secp256k1

Kurva Secp256k1 adalah kurva eliptik yang digunakan dalam kriptografi kunci publik, terutama dalam konteks *blockchain* dan *cryptocurrency* seperti *Bitcoin*. Secp256k1 mengacu pada standar untuk kurva eliptik dengan bentuk matematika yang spesifik yang digunakan untuk menghasilkan pasangan kunci kriptografi.

Kunci privat pada kurva Secp256k1 adalah bilangan bulat 256-bit. Kunci publiknya adalah titik (x, y) pada kurva, dihitung dengan mengalikan kunci privat dengan titik dasar yang telah ditentukan (biasanya disebut sebagai *base point*).

Kurva Secp256k1 memiliki struktur matematika yang didefinisikan oleh persamaan eliptik yaitu

$$y^2 = x^3 + 7$$

di atas bidang lapangan hingga dengan modulus p, di mana p adalah

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 2^0$$

Base point untuk kurva ini dalam bentuk bilangan hexadesimal adalah

G = 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B
16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419
9C47D08F FB10D4B8

2.4 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) adalah metode kriptografi yang telah menjadi standar pengamanan data yang paling luas digunakan di seluruh dunia. *AES* dikenal karena keamanannya yang tinggi dan efisiensinya dalam melindungi informasi sensitif. Metode ini digunakan secara luas dalam berbagai aplikasi, termasuk komunikasi online, penyimpanan data, dan perlindungan informasi penting. *AES* bekerja dengan menggunakan algoritma kunci simetris, yang berarti kunci yang digunakan untuk mengenkripsi dan mendekripsi data adalah sama. Kunci ini harus dijaga dengan sangat rahasia, karena akses ke kunci akan memberikan kemampuan untuk membaca dan mengubah data yang telah dienkripsi.

Salah satu keunggulan *AES* adalah kemampuannya dalam melindungi data dengan tingkat keamanan yang sangat tinggi. Algoritma *AES* bekerja dengan memecah data menjadi blok-blok kecil dan kemudian mengenkripsi setiap blok secara terpisah.

Ini menjadikan *AES* sangat tangguh terhadap serangan brute force, di mana penyerang mencoba semua kombinasi kunci yang mungkin untuk mendekripsi data. *AES* juga memiliki tiga tingkat keamanan yang berbeda berdasarkan panjang kunci yang digunakan: 128-bit, 192-bit, dan 256-bit. Semakin panjang kunci yang digunakan, semakin tinggi tingkat keamanannya. *AES* 256-bit dianggap sebagai tingkat keamanan tertinggi dan sering digunakan dalam pengaturan yang memerlukan tingkat proteksi data paling kuat.

Metode *AES* telah menjadi dasar pengamanan data di banyak aplikasi dan protokol keamanan. Ini digunakan dalam HTTPS untuk melindungi komunikasi web, dalam enkripsi data di perangkat penyimpanan, dan dalam aplikasi keamanan yang lebih tinggi seperti Virtual Private Networks (VPN) dan Perlindungan Data Pribadi (GDPR). *AES* terus menjadi salah satu metode kriptografi paling kuat dan andal yang digunakan di seluruh dunia. Kemampuannya untuk melindungi data dengan tingkat keamanan yang tinggi dan efisiensinya dalam kinerja membuatnya menjadi pilihan yang penting dalam upaya menjaga kerahasiaan dan integritas informasi dalam era digital saat ini.

2.4.1 AES-CBC (Cipher Block Chaining)

AES-CBC (*Advanced Encryption Standard - Cipher Block Chaining)* adalah salah satu mode operasi kriptografi yang digunakan dalam mengenkripsi data, yang memanfaatkan algoritma *AES*. Mode operasi *AES*-CBC adalah salah satu dari beberapa mode yang digunakan dengan *AES* untuk mengenkripsi pesan teks biasa. Ini berfokus pada enkripsi blok data dalam mode berantai untuk memberikan keamanan ekstra.

Cara kerja *AES*-CBC adalah dengan membagi pesan teks biasa menjadi blok-blok data tetap dengan ukuran yang sama, biasanya 128 bit. Setiap blok ini kemudian dienkripsi dengan menggunakan kunci kriptografi *AES* yang sama. Namun, yang membuat *AES*-CBC unik adalah penggunaan "berantai" (chaining). Setiap blok yang dienkripsi kemudian di-XOR (eksklusif OR) dengan blok hasil enkripsi sebelumnya. Ini berarti setiap blok dienkripsi dengan memperhitungkan hasil dari blok sebelumnya, menciptakan hubungan yang berantai.

Kelebihan utama dari *AES*-CBC adalah keamanan dan ketahanannya terhadap serangan pengacauan (bit-flipping) pada pesan yang dienkripsi. Jika hanya satu bit pada pesan teks biasa diubah, maka seluruh hasil enkripsi blok berikutnya akan berubah secara drastis. Ini membuatnya sangat sulit bagi penyerang untuk memanipulasi pesan tanpa diketahui oleh penerima pesan.

Namun, *AES*-CBC juga memiliki beberapa kelemahan. Salah satunya adalah bahwa enkripsi blok-blok data dilakukan secara berurutan, yang berarti tidak ada kemampuan untuk melakukan enkripsi paralel pada blok-blok yang berbeda. Selain itu, *AES*-CBC juga membutuhkan penanganan yang khusus untuk pesan dengan panjang yang tidak tepat kelipatan 128 bit, seperti padding (penambahan bit tambahan pada akhir pesan) untuk menyeimbangkan panjang pesan.

Penting untuk mencatat bahwa *AES*-CBC adalah mode operasi yang banyak digunakan dan dianggap aman ketika diimplementasikan dengan benar. Meskipun begitu, penggunaan yang tidak benar atau kesalahan dalam implementasi dapat mengakibatkan celah keamanan. Oleh karena itu, ketika mengimplementasikan *AES*-CBC, perlu diperhatikan masalah seperti manajemen kunci, pengolahan padding, dan perlindungan dari serangan sisi.

Selain *AES*-CBC, terdapat juga berbagai mode operasi kriptografi lainnya yang dapat digunakan bersama dengan *AES*, seperti *AES*-ECB (Electronic Codebook), *AES*-OFB (Output Feedback), dan *AES*-CTR (Counter). Pemilihan mode operasi yang sesuai harus mempertimbangkan kebutuhan keamanan, kinerja, dan fungsionalitas yang spesifik untuk aplikasi atau skenario penggunaan tertentu.

2.5 Internet of Things (IoT)

Internet of Things (IoT), atau dalam bahasa Indonesia sering disebut sebagai "Internet Hal-Hal," adalah konsep yang merujuk pada jaringan perangkat fisik atau "benda" yang terhubung ke internet dan memiliki kemampuan untuk mengumpulkan, mentransmisikan, dan menerima data. Konsep ini telah mengubah cara kita berinteraksi dengan dunia fisik di sekitar kita dan memiliki dampak yang signifikan dalam berbagai bidang. *IoT* menggabungkan beberapa teknologi utama, termasuk perangkat keras

(hardware) yang terdiri dari sensor dan aktuator, konektivitas nirkabel, serta perangkat lunak (software) yang memungkinkan pengolahan dan analisis data. Ini memungkinkan objek sehari-hari, seperti perangkat rumah tangga, kendaraan, perangkat medis, dan infrastruktur kota, untuk menjadi "terhubung" dan dapat dikendalikan melalui jaringan internet.

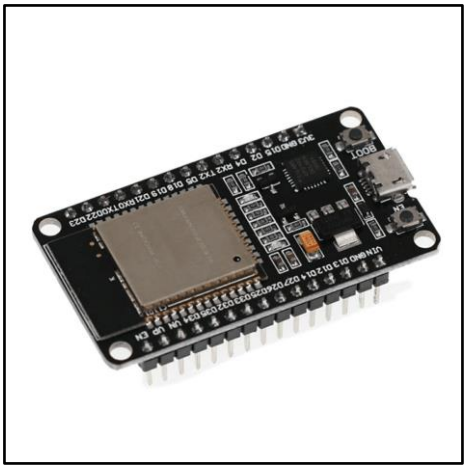
Sejarah *IoT* dapat ditelusuri hingga awal 2000-an ketika konsep ini mulai diperkenalkan. Namun, kemajuan dalam teknologi sensor, konektivitas, dan komputasi, serta penurunan harga perangkat keras, telah memungkinkan pertumbuhan pesat dalam adopsi *IoT*. Perangkat *IoT* dapat digunakan dalam berbagai aplikasi, termasuk:

1) Smart Home: Perangkat *IoT* digunakan untuk mengontrol pencahayaan, pemanasan, pendinginan, keamanan, dan perangkat lainnya di rumah dengan menggunakan aplikasi seluler atau suara.
2) Pemantauan Lingkungan: Sensor *IoT* dapat digunakan untuk memantau kualitas udara, suhu, kelembaban, dan faktor-faktor lingkungan lainnya untuk tujuan pemantauan lingkungan dan peringatan dini.
3) Kesehatan: Perangkat *IoT* digunakan dalam perangkat medis pintar, seperti monitor detak jantung atau alat pelacak kebugaran, untuk memantau dan mengirim data kesehatan.
4) Manufaktur dan Industri: *IoT* digunakan untuk meningkatkan efisiensi dan keamanan dalam operasi manufaktur dan industri dengan pemantauan mesin otomatis dan analisis data real-time.
5) Transportasi Cerdas: Kendaraan terhubung dan sistem transportasi cerdas menggunakan *IoT* untuk meningkatkan keselamatan dan efisiensi dalam perjalanan.

2.6 Mikrokontroller ESP32

ESP32 adalah mikrokontroler yang memiliki dua inti prosesor Xtensa 32-bit LX6 yang kuat dan dapat beroperasi secara independen. Frekuensi prosesor dari mikrokontroller ini dapat bekerja dari 160MHz hingga 240MHz. Memiliki 520 KiB

RAM dan 448 KiB ROM. Ini memberikan kemampuan untuk menjalankan tugas-tugas secara paralel, memungkinkan pengolahan data yang lebih efisien dalam aplikasi *IoT* yang kompleks. Mikrokontroler ini juga dilengkapi dengan berbagai periferal dan antarmuka, termasuk GPIO, UART, SPI, I2C, dan banyak lagi, yang memungkinkan penghubungan dengan berbagai sensor dan perangkat eksternal.



Gambar 2.2 ESP32 (Sumber: www.makerselectronics.com)

Salah satu fitur utama ESP32 adalah kemampuan konektivitas yang luas. Ia mendukung Wi-Fi 802.11 b/g/n, Bluetooth Classic, dan Bluetooth Low Energy (BLE). Ini memungkinkan perangkat ESP32 untuk terhubung ke jaringan Wi-Fi, perangkat Bluetooth, serta komunikasi nirkabel dengan perangkat lain, menjadikannya ideal untuk pengembangan aplikasi *IoT* yang memerlukan konektivitas yang handal.

ESP32 juga memiliki berbagai modul komunikasi dan fitur keamanan yang telah terintegrasi dengan baik, seperti dukungan untuk enkripsi WPA/WPA2, serta kemampuan untuk mengatur akses melalui halaman web yang dihosting di dalam mikrokontroler.

Selain itu, ESP32 didukung oleh komunitas yang besar dan aktif dari pengembang yang terus berkontribusi dalam pengembangan perangkat lunak, dokumentasi, dan proyek open-source yang berhubungan dengan mikrokontroler ini. Ini membuatnya mudah digunakan, dikonfigurasi, dan dikembangkan untuk berbagai aplikasi, dari proyek hobi hingga proyek industri yang lebih besar.

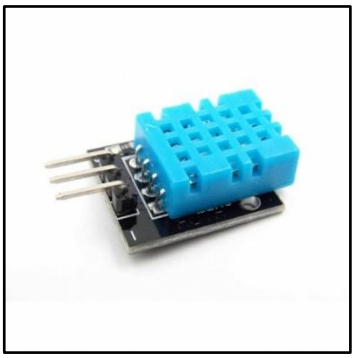
2.7 Sensor

Sensor adalah komponen yang memiliki kemampuan untuk mendeteksi perubahan dalam lingkungan fisik atau kimia, seperti suhu, cahaya, gerakan, tekanan, kelembaban, kecepatan, dan sebagainya. Perangkat sensor ini berfungsi untuk mengubah sinyal dari lingkungan tersebut menjadi sinyal listrik yang dapat diproses oleh komputer atau mikrokontroler. Penggunaan sensor sangat luas dalam berbagai aplikasi *Internet of Things (IoT)*, termasuk dalam bidang kesehatan, industri, smart home, dan smart city. Peran sensor dalam aplikasi *IoT* adalah untuk mengumpulkan data dari lingkungan sekitar dan membantu dalam pengambilan keputusan yang lebih baik dengan memanfaatkan data yang telah terkumpul (Saryazdi, et al., 2019).

2.7.1 DHT11

Sensor DHT11 adalah sensor suhu dan kelembaban digital yang dikembangkan oleh perusahaan Aosong Electronics, yang juga dikenal dengan nama "Aosong." Sensor ini beroperasi berdasarkan prinsip perubahan resistansi pada elemen semikonduktor ketika suhu dan kelembaban berubah. Sensor DHT11 memiliki dua komponen utama: sensor suhu dan sensor kelembaban.

1) Sensor Suhu: Sensor suhu DHT11 menggunakan sebuah termistor (thermistor) untuk mengukur suhu. Termistor adalah perangkat semikonduktor yang resistansinya berubah sesuai dengan suhu. Sensor suhu DHT11 dapat memberikan pembacaan suhu dalam rentang sekitar 0°C hingga 50°C (32°F hingga 122°F) dengan ketelitian sekitar ±2°C (±3.6°F).
2) Sensor Kelembaban: Sensor kelembaban DHT11 menggunakan bahan yang dapat menyerap air untuk mengukur kelembaban. Sensor ini memberikan pembacaan kelembaban dalam rentang sekitar 20% hingga 90% dengan ketelitian sekitar ±5%.

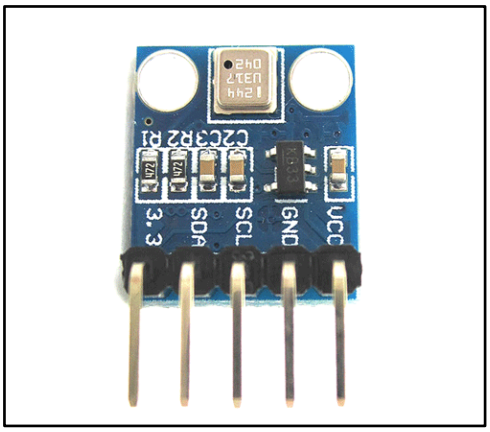


Gambar 2.3 DHT11 (Sumber: www.devobox.com)

Salah satu keunggulan sensor DHT11 adalah kemudahan penggunaannya. Sensor ini biasanya sudah dilengkapi dengan modul sensor yang mencakup sensor itu sendiri, resistor, dan elektronika tambahan yang diperlukan untuk komunikasi dengan mikrokontroler atau perangkat lainnya. Sensor DHT11 biasanya menghasilkan keluaran digital dalam bentuk data suhu dan kelembaban yang mudah diinterpretasikan oleh perangkat pemrosesan data. Sensor DHT11 dapat digunakan dengan berbagai mikrokontroler, seperti Arduino, Raspberry Pi, NodeMCU, dan sebagainya. Ada juga berbagai pustaka (libraries) dan perangkat lunak yang tersedia untuk membaca data dari sensor DHT11, yang memudahkan pengguna untuk mengintegrasikannya dalam proyek-proyek mereka.

2.7.2 BMP180

Sensor BMP180 adalah perangkat sensor digital yang digunakan untuk mengukur tekanan atmosfer dan suhu di sekitar lokasinya. Dikembangkan oleh Bosch Sensortec, sensor ini beroperasi berdasarkan perubahan tekanan atmosfer dengan ketinggian. Dengan teknologi piezoelektrik, BMP180 mampu mengubah perbedaan tekanan menjadi nilai tekanan yang dapat dibaca oleh perangkat eksternal. Selain itu, sensor ini juga dapat mengukur suhu di sekitarnya, yang menjadikannya berguna dalam berbagai aplikasi, termasuk pemantauan cuaca, navigasi, dan pengukuran ketinggian.



Gambar 2.4 BMP180 (Sumber: www.components101.com)

Sensor BMP180 berkomunikasi dengan mikrokontroler melalui antarmuka I2C, memungkinkan perangkat eksternal untuk mengirim permintaan dan menerima data tekanan dan suhu dalam bentuk digital. Dengan keunggulan dalam akurasi, ukuran yang kompak, dan konsumsi daya yang rendah, sensor BMP180 menjadi pilihan yang baik untuk aplikasi portabel dan perangkat bertenaga baterai. Program mikrokontroler Anda dapat diprogram untuk berinteraksi dengan sensor ini, dan data yang diterima dapat digunakan dalam berbagai perhitungan yang relevan sesuai kebutuhan aplikasi Anda. Sensor BMP180 adalah alat yang andal untuk memantau tekanan atmosfer dan suhu dengan akurasi tinggi dalam berbagai pengaturan aplikasi yang memerlukan data presisi.

2.7.3 AJ-SR04M

Sensor AJ-SR04M adalah sensor ultrasonik yang digunakan untuk mengukur jarak antara sensor dan objek di depannya. Sensor ini beroperasi dengan memancarkan gelombang ultrasonik dan mengukur waktu yang diperlukan untuk gelombang tersebut kembali setelah memantul dari objek. Ini memungkinkan sensor untuk menghitung jarak dengan akurasi yang baik. Sensor AJ-SR04M terdiri dari dua komponen utama: pemancar ultrasonik dan penerima ultrasonik. Pemancar menghasilkan gelombang ultrasonik yang dikirimkan ke objek di depan sensor, sementara penerima menerima gelombang tersebut setelah memantul. Waktu yang diperlukan oleh gelombang untuk pergi ke objek dan kembali diukur, dan jarak dihitung berdasarkan waktu tempuh ini.

Gambar 2 5 AJ-SR04M (Sumber: www.tutorials.probots.co.in)

Sensor ini mudah digunakan dan dapat beroperasi dalam berbagai aplikasi, seperti pengukuran jarak, deteksi objek, dan navigasi robot. Komunikasi dengan mikrokontroler biasanya dilakukan melalui antarmuka digital, seperti GPIO atau antarmuka serial. Hasil pengukuran jarak dapat digunakan dalam berbagai aplikasi, seperti menghindari rintangan, menentukan letak objek, atau mengukur jarak antara sensor dan objek tertentu. Keuntungan dari sensor AJ-SR04M meliputi akurasi pengukuran yang baik, respon cepat, serta kemampuan untuk bekerja dalam berbagai kondisi lingkungan. Namun, perlu diingat bahwa performa sensor ini dapat dipengaruhi oleh permukaan dan bahan objek yang diukur, serta kondisi cahaya di sekitarnya. Dalam penggunaan praktis, sensor AJ-SR04M dapat diintegrasikan ke dalam berbagai proyek elektronik dan robotika untuk memungkinkan pengukuran jarak yang akurat. Ini adalah alat yang sangat berguna untuk aplikasi yang memerlukan deteksi jarak dan navigasi.

2.7.4 TS-300B

Sensor kekeruhan cairan TS-300B adalah perangkat sensor yang dirancang khusus untuk mengukur tingkat kekeruhan atau turbiditas dalam air atau cairan lainnya. Turbiditas mengacu pada sejauh mana partikel-padat, mikroba, atau materi lainnya yang tersebar dalam cairan, mengurangi kejernihan atau transparansi cairan tersebut. Sensor ini membantu untuk memahami kualitas air dan dapat digunakan dalam

berbagai aplikasi, seperti pemantauan kualitas air, pengolahan air, penelitian lingkungan, dan banyak lagi.

Sensor kekeruhan cairan TS-300B bekerja dengan mengukur seberapa banyak cahaya yang tersebar atau diserap oleh partikel-partikel dalam cairan. Prinsip kerjanya melibatkan pengiriman cahaya (biasanya cahaya inframerah) melalui sampel cairan dan pengukuran sejauh mana cahaya tersebut tersebar atau diserap oleh partikel dalam cairan. Hasil pengukuran ini kemudian dikonversi menjadi nilai turbiditas, yang biasanya diukur dalam unit Nephelometric Kekeruhan cairan Unit (NTU).

Gambar 2.6 TS-300B (Sumber: www.xcluma.com)

Sensor ini sering digunakan dalam aplikasi pemantauan kualitas air, seperti pemantauan kualitas air minum, sungai, danau, dan pantai. Ini juga penting dalam industri pengolahan air untuk memantau efektivitas penyaringan air dan untuk mengidentifikasi masalah atau kontaminasi dalam air. Selain itu, sensor kekeruhan cairan TS-300B digunakan dalam penelitian lingkungan untuk mengkaji dampak polusi atau perubahan lingkungan terhadap kualitas air.

Keunggulan dari sensor kekeruhan cairan TS-300B adalah kemampuannya untuk memberikan data kualitas air secara cepat dan akurat. Hal ini memungkinkan pengguna untuk mengidentifikasi perubahan dalam turbiditas air, yang dapat menjadi indikator polusi atau gangguan dalam sistem penyaringan air. Selain itu, sensor ini dapat bekerja

secara kontinu atau dalam interval tertentu, memberikan data yang berkelanjutan untuk pemantauan jangka panjang.

Untuk berinteraksi dengan sensor kekeruhan cairan TS-300B, data yang dihasilkan biasanya dapat diakses melalui antarmuka digital, yang memungkinkan pengguna untuk mengakses dan menganalisis data turbiditas. Sensor ini juga dapat diintegrasikan dengan sistem pemantauan air yang lebih besar atau sistem kendali otomatis untuk mengambil tindakan sesuai dengan perubahan kualitas air.

Dalam kesimpulan, sensor kekeruhan cairan TS-300B adalah alat yang sangat berharga dalam pemantauan dan pengukuran kualitas air, dengan aplikasi yang mencakup air minum, lingkungan, dan pengolahan air. Sensor ini memberikan data turbiditas yang akurat dan dapat diandalkan, membantu dalam menjaga kualitas air yang layak dan lingkungan yang sehat.

2.8 LoRa (Long Range)

LoRa adalah singkatan dari "Long Range" yang merupakan teknologi komunikasi nirkabel yang memungkinkan transmisi data dalam jarak yang sangat jauh. Teknologi ini didasarkan pada modulasi *Chirp Spread Spectrum (CSS)* dan biasanya digunakan dalam konteks *Internet of Things (IoT)* serta komunikasi jarak jauh. Keunggulan utama *LoRa* termasuk jangkauan komunikasi yang luas, konsumsi daya yang rendah, dan ketahanan terhadap gangguan. Hal ini memungkinkan perangkat *LoRa* untuk berkomunikasi dalam jarak beberapa kilometer atau lebih tanpa perlu daya yang besar, menjadikannya ideal untuk aplikasi seperti pemantauan lingkungan, manajemen aset, *smart city*, dan banyak lagi.

Gambar 2.7 LoRa (Sumber: www.biggo.id)

Teknologi *LoRa* bekerja pada berbagai rentang frekuensi radio yang telah ditentukan dan diatur sesuai dengan regulasi di berbagai wilayah. Selain itu, penggunaan modulasi CSS memungkinkan *LoRa* untuk bertahan dalam lingkungan perkotaan yang penuh noise dan interferensi. *LoRa* sering diimplementasikan dalam jaringan nirkabel yang disebut *LoRa*WAN (Long Range Wide Area Network) yang memungkinkan perangkat *LoRa* untuk terhubung ke gateway dan mengirimkan data ke server pusat. Data ini kemudian dapat diakses, dianalisis, dan digunakan untuk berbagai aplikasi, termasuk pengambilan keputusan yang cerdas.

Dengan kemampuannya untuk mengatasi tantangan konektivitas jarak jauh, efisiensi daya, dan ketahanan terhadap gangguan, *LoRa* telah menjadi pilihan utama dalam banyak proyek *IoT* dan komunikasi nirkabel yang memerlukan jangkauan yang luas dan konsumsi daya yang rendah. Teknologi ini terus berkembang dan berkontribusi dalam menghadirkan solusi terhubung yang lebih efisien.

2.9 Penelitian Relevan

Berikut ini beberapa penelitian yang berkaitan dengan penelitian ini, yaitu:

1) Penelitian terdahulu yang dilakukan oleh Nadeem Chanin dan Abeer Mansour yang berjudul *"Improving the IoT and Cloud Computing integration using Hybrid Encryption"* (2023) bertujuan untuk meningkatkan integrasi antara *IoT* dan Cloud Computing dengan menerapkan teknologi enkripsi hybrid. Hasil penelitian ini

menunjukkan bahwa penggunaan enkripsi hybrid dalam integrasi *IoT* dan Cloud Computing dapat meningkatkan tingkat keamanan secara signifikan. Ini dapat membantu melindungi data yang dikirim dari perangkat *IoT* ke cloud, yang seringkali berisi informasi penting.

2) Penelitian terdahulu yang dilakukan oleh Mohammad Al-Mashhadani dan Mohamed Shujaa yang berjudul *"IoT Security Using AES Encryption Technology based ESP32 Platform"* (2022) mengevaluasi dan mengimplementasikan teknologi enkripsi *AES* sebagai solusi untuk meningkatkan keamanan dalam konteks *IoT*, dengan menggunakan platform ESP32 sebagai contoh implementasi. Penelitian ini menunjukkan bahwa dengan mengimplementasikan *AES* dalam perangkat ESP32, data yang dikirim dan diterima oleh perangkat *IoT* dapat dienkripsi dengan baik, sehingga melindungi informasi yang dikirim melalui jaringan *IoT* dari potensi ancaman keamanan seperti penyadapan atau manipulasi data.
3) Penelitian terdahulu yang dilakukan oleh Huiwei Yang yang berjudul *"Application of Hybrid Encryption Algorithm in Hardware Encryption Interface Card"* (2022) mengevaluasi dan menerapkan algoritma enkripsi hybrid dalam sebuah kartu antarmuka enkripsi perangkat keras. Kartu ini mungkin digunakan sebagai perangkat tambahan dalam sistem komputer untuk mengamankan data yang disimpan atau data yang dikirim melalui jaringan. Hasil penelitian ini menunjukkan bahwa penggunaan algoritma enkripsi hybrid dalam kartu antarmuka enkripsi perangkat keras dapat menjadi solusi yang efektif untuk melindungi data yang sensitif dan meningkatkan tingkat keamanan dalam lingkungan komputasi.
4) Penelitian terdahulu yang dilakukan oleh Meryam Saad Fadhi, Alaa Kadhim Farhan dan Mohammad Natiq Fadhil yang berjudul *"A lightweight AES Algorithm Implementation for Secure IoT Environment"* (2021) mengimplementasikan algoritma *Advanced Encryption Standard (AES)* yang memiliki tingkat keamanan yang tinggi namun juga efisien dalam lingkungan *Internet of Things (IoT)*. Hasil penelitian menunjukkan bahwa implementasi versi ringan dari *AES* dapat berhasil

dilakukan dengan efisien di perangkat *IoT* yang memiliki keterbatasan sumber daya, seperti daya dan pemrosesan.

5) Penelitian terdahulu yang dilakukan oleh Omid Mahdi Ebadati E., Farshad Eshghi , dan Amin Zamani yang berjudul *"A Hybrid Encryption Algorithm for Security Enhancement of Wireless Sensor Networks: A Supervisory Approach to Pipelines"* (2020) mengembangan algoritma enkripsi hybrid untuk meningkatkan keamanan jaringan sensor nirkabel *(Wireless Sensor Networks atau WSN)*. Hasil penelitian menunjukkan bahwa penggunaan algoritma enkripsi hybrid dapat meningkatkan tingkat keamanan dalam konteks WSN yang sering digunakan dalam aplikasi pengawasan.

BAB 3
ANALISIS DAN PERANCANGAN

3.1 Analisis Sistem

Analisis sistem merupakan tahap yang penting dalam pengembangan suatu sistem, di mana sistem yang kompleks dipecah menjadi elemen-elemen yang lebih sederhana untuk mempermudah pengenalan masalah yang ingin diatasi. Dari hasil identifikasi yang dilakukan selama analisis sistem, akan diperoleh gambaran tentang bagaimana komponen-komponen tersebut terhubung satu sama lain, yang akan menjadi dasar dalam merancang sistem. Proses analisis sistem melibatkan serangkaian tahap yang harus dijalani secara berurutan guna memahami kebutuhan dan struktur sistem yang akan dikembangkan secara menyeluruh.

3.1.1 Analisis Masalah

Salah satu permasalahan utama yang dihadapi dalam komunikasi *LoRa* adalah kurangnya keamanan data. Keamanan data adalah aspek yang sangat penting dalam konteks pengiriman data, terutama ketika data tersebut berisi informasi yang sensitif atau berdampak besar, seperti data kesehatan, lingkungan, atau keamanan. Kekurangan keamanan data dapat berpotensi mengakibatkan pelanggaran privasi, manipulasi data, dan risiko keselamatan. Komunikasi *LoRa* sering kali menggunakan frekuensi terbuka, yang memungkinkan akses yang mudah oleh pihak yang tidak berwenang ke data yang dikirim melalui jaringan *LoRa*. Hal ini menjadi sumber kerentanan serius, karena data yang tidak dienkripsi dapat dengan mudah disadap dan dimanipulasi oleh pihak yang tidak berwenang.

Dalam upaya meningkatkan keamanan data dalam komunikasi *LoRa*, penelitian ini mengusulkan penggunaan *Hybrid Cryptosystem*. Pendekatan ini menggabungkan dua metode kriptografi, yaitu *Elliptic Curve Cryptography (ECC)* dan *Advanced Encryption Standard (AES)*, untuk menciptakan tingkat keamanan yang lebih tinggi. Namun, tantangan yang timbul adalah bagaimana mengintegrasikan dan mengimplementasikan *Hybrid Cryptosystem* dengan efektif dalam lingkungan komunikasi *LoRa*. Keterbatasan daya dan sumber daya adalah hal yang umum dalam

perangkat *Internet of Things (IoT)*. Oleh karena itu, pemilihan metode kriptografi harus memperhitungkan efisiensi penggunaan daya dan sumber daya. Pilihan *ECC* dan *AES* dalam *Hybrid Cryptosystem* adalah upaya untuk mempertimbangkan keterbatasan ini.

Keamanan data dalam komunikasi *LoRa* memiliki dampak besar pada perkembangan *Internet of Things (IoT)*. Kekurangan keamanan dapat menghambat adopsi dan pertumbuhan *IoT* di berbagai sektor. Oleh karena itu, pengembangan solusi keamanan yang efektif untuk komunikasi *LoRa* menjadi penting untuk mendukung perkembangan berkelanjutan dalam *IoT*.

3.1.2 Analisis Kebutuhan

Analisis kebutuhan adalah tahap yang yang terbagi menjadi dua bagian, yakni analisis kebutuhan yang bersifat fungsional dan analisis kebutuhan yang bersifat non-fungsional. Dalam proses tahap ini, memahami seluruh kebutuhan sistem yang diperlukan untuk mencapai tujuan yang diinginkan menjadi hal yang sangat penting. Analisis kebutuhan fungsional berkaitan dengan identifikasi fitur dan fungsi yang harus ada dalam sistem, sedangkan analisis kebutuhan non-fungsional membahas aspek-aspek seperti kinerja, keamanan, kehandalan, dan skalabilitas sistem. Dengan menjalankan analisis kebutuhan secara menyeluruh, akan memastikan bahwa sistem yang akan dibangun mampu memenuhi semua kebutuhan yang ada dan mencapai tujuan yang telah ditetapkan.

1) Kebutuhan Fungsional

   Kebutuhan fungsional adalah elemen kunci yang perlu dipenuhi untuk memastikan kelancaran dalam proses pengembangan sistem. Dalam konteks penelitian ini, terdapat sejumlah kebutuhan fungsional yang menjadi fokus utama. Kebutuhan tersebut mencakup:

   a. Sistem mempunyai kemampuan untuk menghasilkan shared secret dari private key dan public key yang dibagikan menggunakan algoritma *Elliptic Curve Cryptography (ECC)*.
   b. Sistem dapat mengenkripsi plaintext berupa format json menggunakan algoritma *AES*.

c. Sistem dapat mendekripsi ciphertext yang diterima menjadi bentuk semula dengan menggunakan algoritma *AES*.
d. Sistem memiliki sensor-sensor sebagai data yang akan diamankan menggunakan algoritma *AES*.
e. Sistem memiliki modul *LoRa* sebagai protocol komunikasi antar mikrokontroller.
f. Sistem memiliki mikrokontroller ESP32 yang berfungsi untuk melakukan proses pembacaan sensor, pengiriman data, pengamanan data dan eksekusi logika program.

2) Kebutuhan Non Fungsional

Kebutuhan non-fungsional adalah kebutuhan yang berperan sebagai pendukung utama dalam menjaga kelancaran operasi sistem. Dalam penelitian ini, sejumlah kebutuhan non-fungsional perlu dipertimbangkan. Beberapa di antaranya mencakup:

a. Performa

Sistem dapat menampilkan hasil proses enkripsi plaintext dan dapat mengembalikan ciphertext menjadi plaintext asli melalui proses dekripsi.

b. Kontrol

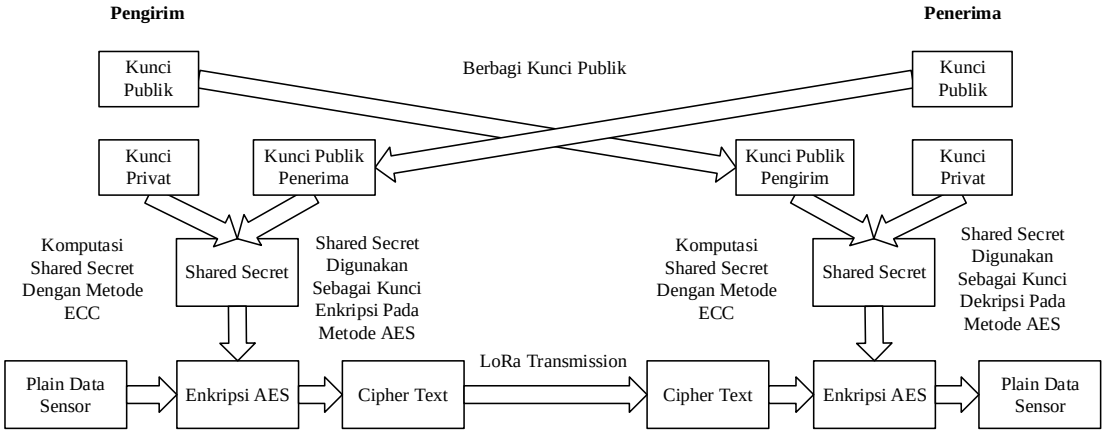
Sistem dapat menampilkan pesan peringatan kesalahan (error message) apabila ada kesalahan pada sistem.

c. Kualitas

Sistem dapat menghasilkan output yang benar dan akurat dalam proses berbagi kunci, enkripsi dan dekripsi.

3.1.3 Arsitektur Umum

Arsitektur umum adalah representasi visual dari cara sistem beroperasi secara keseluruhan. Ilustrasi arsitektur umum sistem ini dapat ditemukan dalam gambar di bawah ini:



Gambar 3.1 Arsitektur Umum

Penjelasan alur proses arsitektur umum pada gambar di atas adalah sebagai berikut:

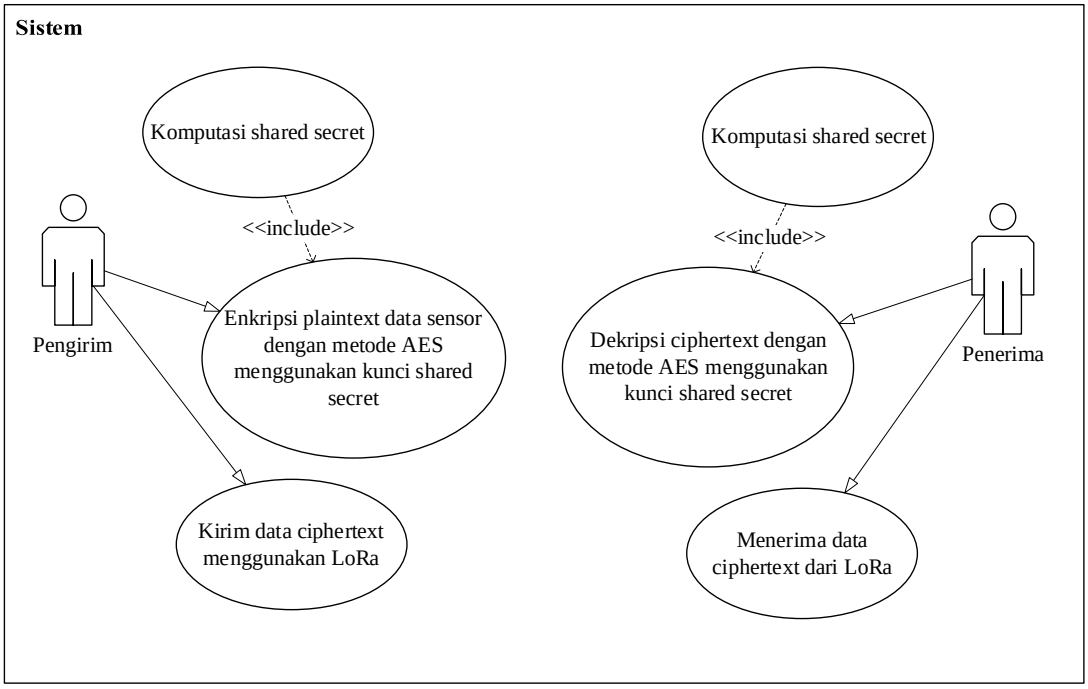
1) Pengirim dan penerima saling berbagi kunci publik, agar dapat mengkomputasi shared secret. Shared secret diperoleh dengan dari kombinasi kunci privat dan kunci publik yang diterima menggunakan metode *ECC*.
2) Pengirim membaca data dari semua sensor, data yang terbaca lalu dienkripsi dengan metode *AES* sehingga menghasilkan cipher text. Enkripsi pada *AES* menggunakan shared secret sebagai kunci enkripsi.
3) Selanjutnya cipher text hasil enkripsi data sensor tadi tadi dikirim ke penerima melalui jaringan *LoRa*.
4) Berikutnya penerima menangkap data yang dikirim melalui frekuensi *LoRa* yang sama, yang mana data tersebut berupa ciphertext.
5) Cipher text yang diterima tersebut dapat didekripsi menggunakan metode *AES* dengan shared secret yang telah dikomputasi tadi sebagai kunci dekripsi.
6) Hasil dari dekripsi akan valid jika shared secret antara pengirim dan penerima sama.

3.2 Pemodelan Sistem

Pemodelan sistem yang akan digunakan adalah use case diagram, activity diagram, dan sequence diagram.

3.2.1 Use Case Diagram

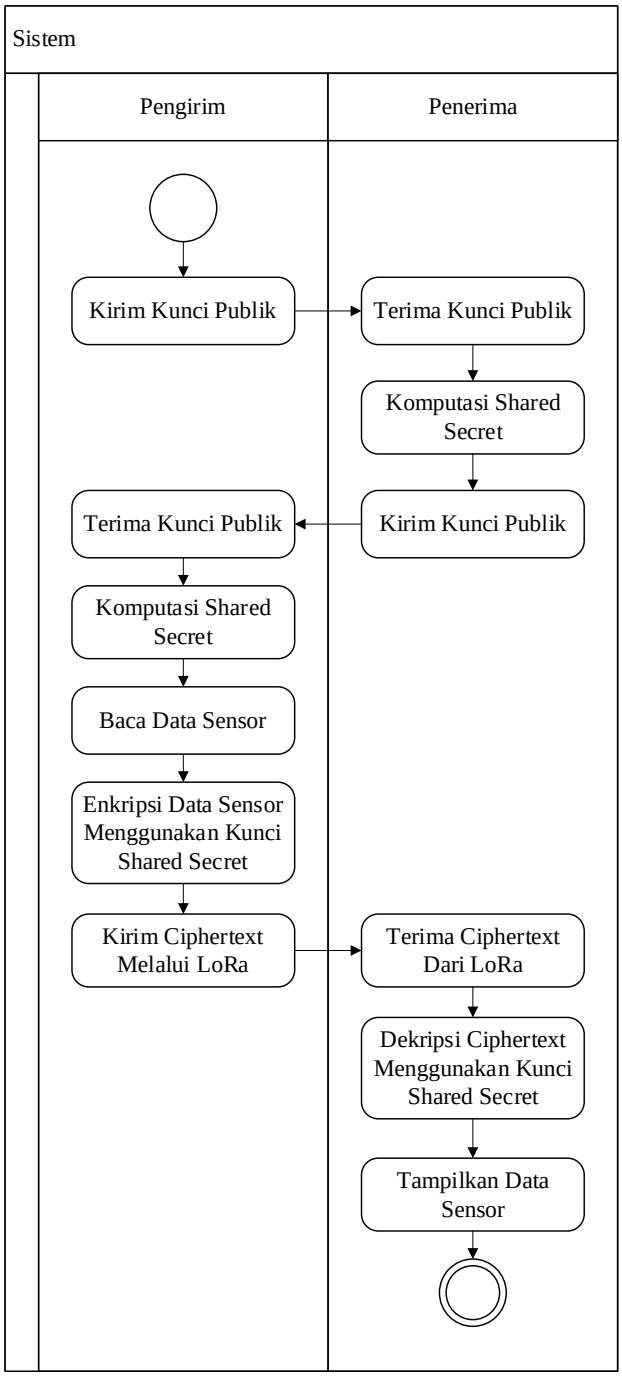
Use case diagram adalah diagram yang menggambarkan interaksi dari aktor yang terlibat dengan sistem. Interaksi ini menjelaskan apa saja yang dapat dilakukan oleh masing-masing aktor. Use case diagram pada sistem ditunjukkan pada gambar berikut:



Gambar 3.2 Use Case Diagram

3.2.2 Activity Diagram

Activity Diagram memberikan gambaran alur kerja sistem secara berurutan dari awal hingga akhir. Activity diagram yang dibangun ditunjukkan pada gambar berikut:

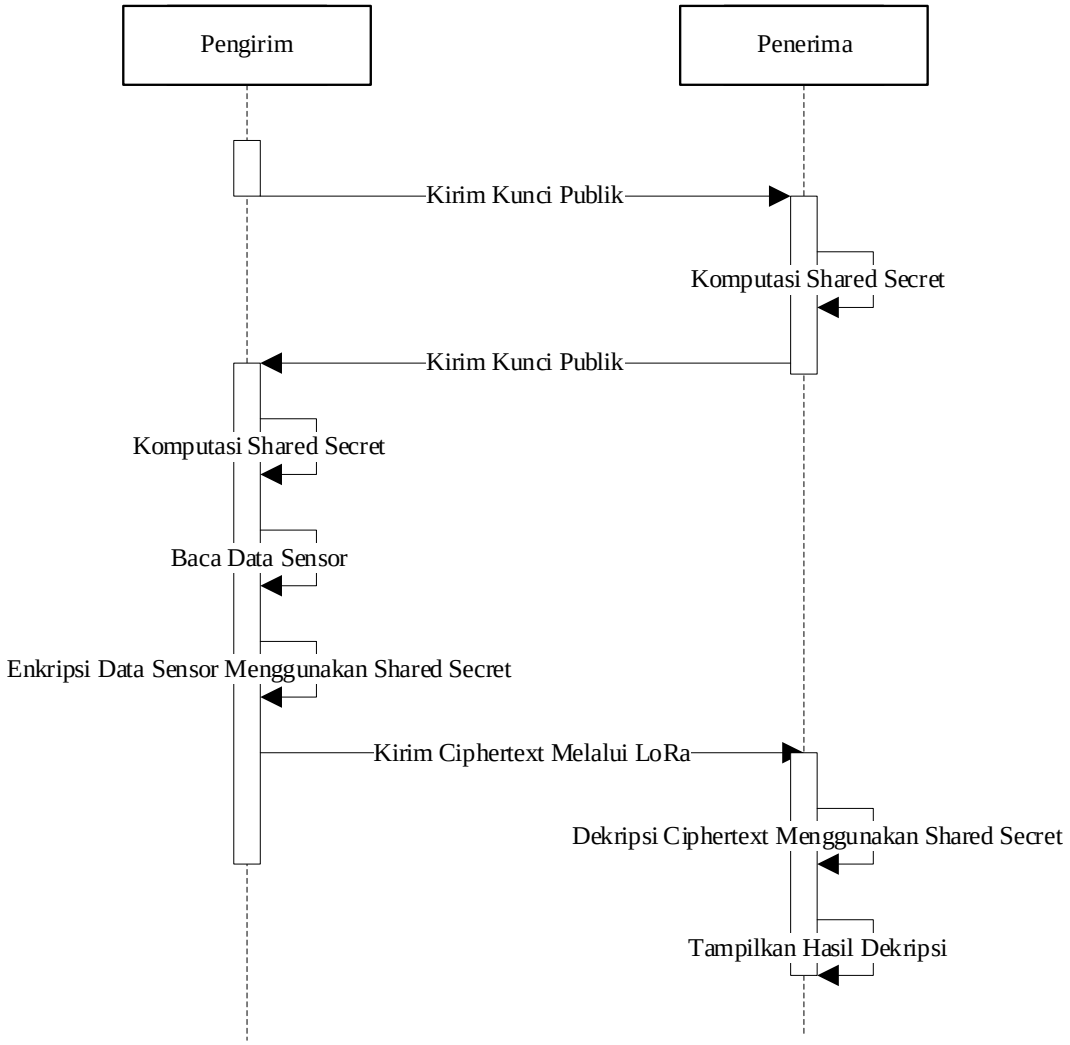


***Gambar 3.3* Activity Diagram**

Berdasarkan activity diagram di atas, dijelaskan aktivitas interaksi pengirim dan penerima. Dimulai dengan saling berbagi kunci publik dan komputasi shared secret pada pengirim dan penerima. Lalu proses enkripsi data sensor menggunakan shared

secret yang kemudian dikirim melalui *LoRa* kepada penerima oleh pengirim. Selanjutnya data ciphertext yang diterima melalui *LoRa* oleh penerima didekripsi menjadi bentuk semula menggunakan shared secret dan ditampilkan ke *console*.

3.2.3 Sequence Diagram



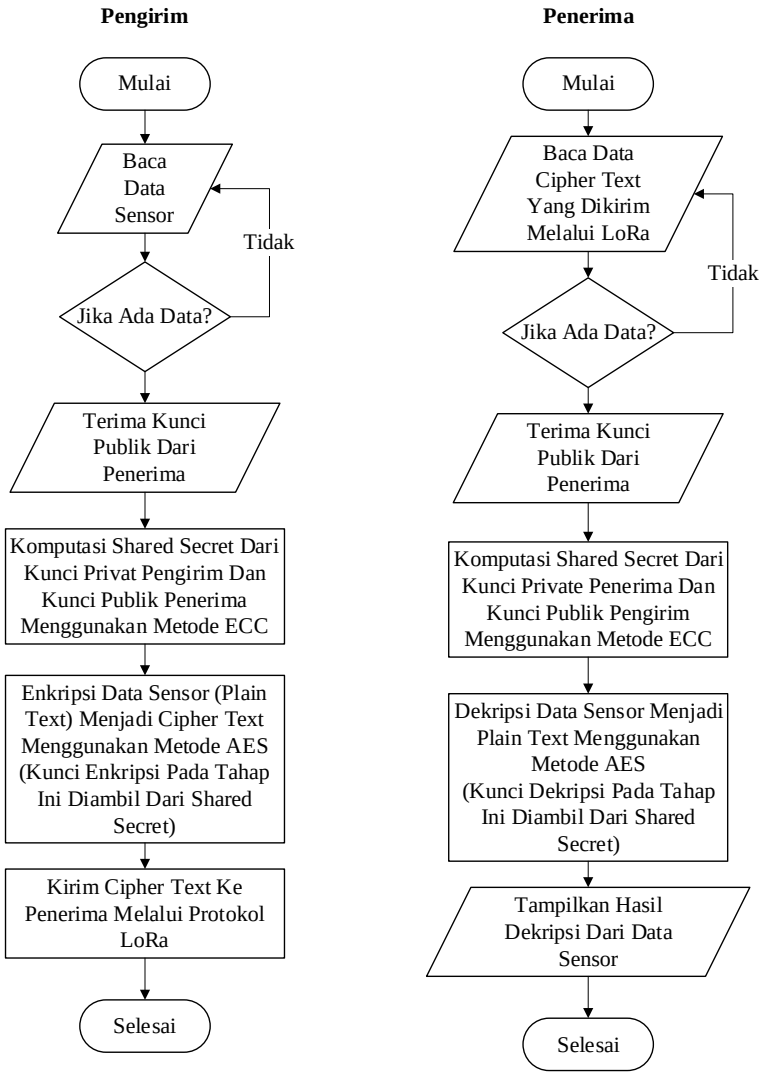
Gambar 3.4 Sequence Diagram

Dari alur komunikasi sistem yang ditunjukkan pada sequence diagram, dimulai dengan pengirim dan penerima yang saling berbagi kunci publik dan mengkomputasi shared secret. Selanjutnya, mengenkripsi data sensor yang dibaca menggunakan kunci

shared secret, ciphertext ini dikirimkan ke penerima melalui *LoRa*. Pada penerima, ciphertext yang diterima melalui *LoRa* di dekripsi menggunakan shared secret lalu hasil dekripsi berupa data sensor tersebut ditampilkan ke *console*.

3.3 Flowchart

Flowchart adalah diagram yang menggambarkan langkah-langkah yang diperlukan untuk merepresentasikan suatu program menggunakan simbol dan garis. Hal ini bertujuan untuk mempermudah pemahaman dan implementasi program ke dalam bahasa pemrograman.



Gambar 3.5 Flowchart Sistem

Pada gambar di atas menunjukkan gambaran umum proses sistem secara keseluruhan dari proses pembacaan sensor, berbagi kunci publik, komputasi shared secret, enkripsi, dekripsi dan menampilkan output dari sistem.

3.4 Perancangan Sistem

Penelitian ini dirancang dengan sistem yang terbagi menjadi dua bagian, yaitu perancangan perangkat keras dan perangkat lunak. Perangkat keras dikonstruksi dengan menggunakan komponen elektronik yang disusun sedemikian rupa sehingga membentuk sebuah sistem elektronika yang terpadu. Sementara itu, perangkat lunak dikembangkan untuk membuat kode program yang bertugas mengirimkan data hasil pembacaan sensor, proses enkripsi dan proses dekripsi data. Data ini kemudian ditampilkan pada *console*.

3.4.1 Peralatan Dan Bahan

1) Peralatan

   Peralatan yang digunakan dalam perancangan sistem ini adalah solder, tang potong, gunting, obeng, dan gergaji.

2) Bahan

   Bahan yang digunakan dalam perancangan sistem ini adalah pada tabel berikut:

Tabel 3.1 Daftar Bahan

Bahan	Keterangan
Mikrokontroller ESP32	2 Buah
Sensor DHT11	1 Buah
Sensor BMP180	1 Buah
Sensor AJ-SR04M	1 Buah
Sensor TS-300B	1 Buah
Lampu Led	2 Buah
Push Button	2 Buah
LCD 1602 I2C	1 Buah
Kabel Jumper	Secukupnya

3.4.2 Perancangan Hardware

Perancangan hardware merupakan perancangan untuk koneksi pengkabelan antara hardware yang satu dengan yang lainnya dan konfigurasi frekuensi yang digunakan pada *LoRa*.

1) Perangkat Pengirim

a. Koneksi Sensor DHT11 Ke Mikrokontroller ESP32

Tabel 3.2 Koneksi Sensor DHT11 Ke Mikrokontroller ESP32

Pin Sensor DHT11	**Pin ESP32**
GND	GND
VCC	3.3V
Data	GPIO2

b. Koneksi Sensor BMP180 Ke Mikrokontroller ESP32

Tabel 3.3 Koneksi Sensor BMP180 Ke Mikrokontroller

Pin Sensor BMP180	Pin ESP32
GND	GND
VCC	3.3V
SDA	GPIO21
SCL	GPIO22

c. Koneksi Sensor AJ-SR04M Ke Mikrokontroller ESP32

Tabel 3.4 Koneksi Sensor AJ-SR04M Ke Mikrokontroller

Pin Sensor AJ-SR04M	Pin ESP32
GND	GND
VCC	3.3V
Trig	GPIO5
Echo	GPIO17

d. Koneksi Sensor TS-300B Ke Mikrokontroller ESP32

Tabel 3.5 Koneksi Sensor TS-300B Ke Mikrokontroller

Pin Sensor TS-300B	Pin ESP32
GND	GND
VCC	3.3V
Data Analog	GPIO32

e. Koneksi *LoRa* Ke Mikrokontroller ESP32

Tabel 3.6 Koneksi LoRa Ke Mikrokontroller (Pengirim)

Pin *LoRa*	Pin ESP32
GND	GND
VCC	3.3V
M0	GND
M1	GND
RXD	GPIO19
TXD	GPIO18

f. Koneksi LED Ke Mikrokontroller ESP32

Tabel 3.7 Koneksi LED Ke Mikrokontroller (Pengirim)

Pin LED	Pin ESP32
Anoda	GPIO16
Katoda	GND

g. Koneksi *Push Button* Ke Mikrokontroller ESP32

Tabel 3.8 Koneksi Push Button Ke Mikrokontroller (Pengirim)

Pin Push Button	Pin ESP32
PIN1	3.3V
PIN2	GPIO13

h. Konfigurasi LoRa

Tabel 3.9 Konfigurasi LoRa (Pengirim)

Frekuensi	868 MHz
UART Baud Rate	9600
Spread Factor	7
RSSI	-120dBm

2) Perangkat Penerima

a. Koneksi LCD 1602 I2C Ke Mikrokontroller ESP32

Tabel 3.10 Koneksi LCD 1602 I2C Ke Mikrokontroller

Pin Sensor BMP180	Pin ESP32
GND	GND
VCC	3.3V
SDA	GPIO16

SCL	GPIO17

b. Koneksi *LoRa* Ke Mikrokontroller ESP32

Tabel 3.11 Koneksi LoRa Ke Mikrokontroller (Penerima)

Pin *LoRa*	Pin ESP32
GND	GND
VCC	3.3V
M0	GND
M1	GND
RXD	GPIO19
TXD	GPIO18

c. Koneksi LED Ke Mikrokontroller ESP32

Tabel 3.12 Koneksi LED Ke Mikrokontroller ESP32 (Penerima)

Pin LED	Pin ESP32
Anoda	GPIO33
Katoda	GND

d. Koneksi Push Button Ke Mikrokontroller ESP32

Tabel 3.13 Koneksi Push Button Ke Mikrokontroller (Penerima)

Pin Push Button	Pin ESP32
PIN1	3.3V
PIN2	GPIO34

e. Konfigurasi *LoRa*

Tabel 3.14 Konfigurasi LoRa (Penerima)

Frekuensi	868 MHz
UART Baud Rate	9600
Spread Factor	7
RSSI	-120dBm

3.4.3 Perancangan Program

Perancangan program merupakan perancangan untuk pembuatan program yang akan dijalankan oleh mikrokontroller perangkat secara terus menerus (looping).

1) Perangkat Pengirim

```
Deklarasi:
private_key, public_key_pengirim, shared_secret,
public_key_penerima, data_sensor, ciphertext
Algoritma:
Send_LoRa(public_key_pengirim)
While shared_secret is null then
    Read(public_key_penerima)
    Calculate_Shared_Secret(public_key_penerima)
While True then
    Read(data_sensor)
    ciphertext <- Encrypt(data_sensor)
    Send_LoRa(ciphertext)
```

2) Perangkat Penerima

```
Deklarasi:
private_key,   public_key_pengirim,   shared_secret,
public_key_penerima, data_sensor, ciphertext
Algoritma:
Send_LoRa(public_key_penerima)
While shared_secret is null then
    Read(public_key_pengirim)
    Calculate_Shared_Secret(public_key_pengirim)
While True then
    ciphertext <- Read_LoRa()
    data_sensor <- Decrypt(ciphertext)
    Print(data_sensor)
```

BAB 4
IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi Sistem

Proses implementasi sistem meliputi beberapa tahapan implementasi, yaitu penerapan dan penggabungan sensor, LCD, push button dan menjalankan program yang telah dirancang sebelumnya pada mikrokontroller.

4.1.1 Implementasi Perancangan Perangkat Pengirim

Implementasi perancangan perangkat pengirim pada sistem ini ialah merancang perangkat yang berfungsi sebagai pengirim data sensor kepada perangkat penerima di mana data sensor tersebut akan dikirim dalam bentuk data yang dienkripsi (ciphertext).

Gambar 4.1 Implementasi Perancangan Perangkat Pengirim

4.1.2 Implementasi Perancangan Perangkat Penerima

Implementasi perancangan perangkat penerima pada sistem ini ialah merancang perangkat yang berfungsi sebagai penerima data sensor yang dikirim oleh perangkat pengirim di mana data sensor tersebut diterima dalam bentuk ciphertext. Untuk mendapatkan isi data sebenarnya, perangkat penerima akan melakukan proses dekripsi pada data ciphertext yang diterima tersebut.

Gambar 4.2 Implementasi Perancangan Perangkat Penerima

4.2 Pengujian Sistem

Tahap ini berisi percobaan dan cara kerja alat yang telah selesai dirancang serta pengecekan apakah data yang dikirim dan diterima valid atau tidak.

4.2.1 Pengujian Komputasi Shared Secret

1) Perangkat Pengirim

```
Sedang Menerima Kunci Publik..
Kunci Publik Diterima..
Durasi Waktu Pengiriman Data : 2.000359 Detik
{'public_key': {'y': 'b7c52588d95c3b9aa25b0403f1eef75702e84bb7597aabe663b82f6f04ef2777
', 'x': 'fb9256390268e7f95867352cd4e5659872bb8c7c988ec9b13981f4d526552401'}}
Shared Secret : 21d5d9df8ef361d76bdadd61d805844162d3d4efc5c56191759636378a32d193
```

Gambar 4.3 Pengujian Komputasi Shared Secret (Pengirim)

2) Perangkat Penerima

Gambar 4.4 Pengujian Komputasi Shared Secret (Penerima)

Dari hasil pengujian komputasi shared secret di atas, perangkat pengirim dan penerima berhasil menghasilkan shared secret yang sama.

4.2.2 Pengujian Enkripsi Data Sensor Pada Perangkat Pengirim

Gambar 4.5 Pengujian Enkripsi Data Sensor Pada Perangkat Pengirim

Dari hasil pengujian enkripsi data sensor di atas, perangkat pengirim berhasil mengenkripsi data sensor menggunakan shared secret.

4.2.3 Pengujian Dekripsi Ciphertext Pada Perangkat Penerima

Gambar 4.6 Pengujian Dekripsi Ciphertext Pada Perangkat Penerima

Dari hasil pengujian dekripsi data ciphertext di atas, perangkat penerima berhasil mendekripsi ciphertext menggunakan shared secret dan menghasilkan output data sensor.

4.2.4 Pengujian Tampilan Hasil Dekripsi Data Sensor Pada LCD

Gambar 4.7 Pengujian Tampilan Hasil Dekripsi Data Sensor Pada LCD

4.2.5 Pengujian Penambahan Random String Pada Proses Enkripsi

Proses enkripsi di bawah dilakukan menggunakan kunci dan IV yang sama yaitu:

Kunci:

57cfde89a8614f3d1a3b556fab62a42684f5027d292b13f58266c5fce1e84538

IV: b4d5238a7aa4a6cbfdd75ee535eb9ed5

1) Tanpa Random String

Tabel 4.1 Pengujian Enkripsi Data Tanpa Random String Tambahan

Plaintext	Ciphertext
{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.159, "satuan": "hPa"}, "suhu": {"nilai": 29.45461, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.88422, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.8054, "satuan": "cm"}, "waktu": "17/11/2023 02:00:14"}	29011bf88f62027017bb2eb14d5e7 6694b7aee640241c3ea186dcc99a8f 8e9567169d6df988e2caec6b7edad7 2a5158de4de60b6cc1e011ab0ccad7 f557974ec0730f58af9dcd03a892e3 8b470eebe951079ff69c1e6ec75acc 2c20dc240da2052d62c557f368bf94 07c2c92e5eaebe2b19b2ae1cbd2216 7d92432f1a1cef1a481385863d174a 46999086608471ef397ef3a3058dc5 6c1ccad647e21a44fff32fe76b8d8c3 a14315a815f4495367fc02f91c0492 73ceabe3c7b1bc453eebaac5468e79 750762c7b9a1006c6ba2eb461857d 8bff6e08a3715b7f6772106dcc8c76 2fa19dacbf2f8953c878572619997f 3a4f994f489c233c3bb37124f7acb4 57b5ac276c6dae8511a678ccc3179 22bb746cc9f8b1f85094e0af86cdbe 4a44eede178291e352918636ae9cb 4c6d9e890d18b1a35449d32aeffa05 9db202e248e4cfac48bb16cc2d6526 55897ace90ef7bb80b92ded1a61e21 b4ebab78ad1e5c09dc56abdf3daede b5b12899952a551457eb6c6dadcee 310510d30b4709fe0544bf11f82215 6593fb557167150a6e5876e0

{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.106, "satuan": "hPa"}, "suhu": {"nilai": 29.43684, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 51.3084, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.6339, "satuan": "cm"}, "waktu": "17/11/2023 02:00:32"}	29011bf88f62027017bb2eb14d5e76694b7aee640241c3ea186dcc99a8f8e9567169d6df988e2caec6b7edad72a5158de4de60b6cc1e011ab0ccad7f557974ec0730f58af9dcd03a892e38b470eebe951079ff69c1e6ec75acc2c20dc240da2052d62c557f368bf9407c2c92e5eaebe2b19b2ae1cbd22167d92432f1a1cef1a481385863d174a46999086608471ef397ef3a3058dc56c1ccad647e21a44fff32fe76b8d8c3a14315a815f4495367fc02694a6865f5fb605633967a728c4eefa739255189751de59c97a06b40535245f066445ac5ec65e15ded9dc6c39b03278a4bf1a192b1fb65ead99ffa34113b91045ff2080e4bf0cac1318e09c9dca14915fc41a46f3111b6134b00aef3839bafdca7f09454c146475109e66e33509e30f51ad5da2546ad648fecd91fc2201e4e1e1c8b93167c2241561c01cfc2cbd31d3755dbcbecb79c7bcfe8e3a6b48bb93338c84d94bcca280bb19b0909cdf85cb0253a0e5ba7b75797f48453d03d2368ad9ff0ad65140d24e54358838693606c3786d01a54a0a3cd2a930fb52a1af63898ed
{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.165, "satuan": "hPa"}, "suhu": {"nilai": 29.43684, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.83342, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.5995, "satuan": "cm"}, "waktu": "17/11/2023 02:00:50"}	29011bf88f62027017bb2eb14d5e76694b7aee640241c3ea186dcc99a8f8e9567169d6df988e2caec6b7edad72a5158de4de60b6cc1e011ab0ccad7f557974ec0730f58af9dcd03a892e38b470eebe951079ff69c1e6ec75acc2c20dc240da2052d62c557f368bf9407c2c92e5eaebe2b19b2ae1cbd22167d92432f1a1cef1a481385863d174a46999086608471ef397ef3a3058dc56c1ccad647e21a44fff32fe76b8d8c3a14315a815f4495367fc02a44061b378203dd2c9318866af64d7973b3521897da6fa10568d122b5918c8cc07c42e09b85fcf1fc0170df19d28ca0506011ce785be80eb5763aa5785bcbfe17b5c514236754348953c7f0c2e1

	28ff45ad56ceb360d312b3872b106 73037870a3f2da748bfec5ab681eb8 ad4107dac337f18db2683c0cba55ba 614ef4231f700d2d7ae54caead057e 656fa5adbde9f2f8f0fb5c48c6f3b26 3fa253241d519739b957ea0b459fde bb0936d91e2375ec42126d132a120 986ffad68aa095a93fdb8e883b6c29 ab69b3669fbbc67429552b55378db 627431bc6778570a0823fbcb4
{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.132, "satuan": "hPa"}, "suhu": {"nilai": 29.42499, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 51.09703, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.7711, "satuan": "cm"}, "waktu": "17/11/2023 02:01:08"}	29011bf88f62027017bb2eb14d5e7 6694b7aee640241c3ea186dcc99a8f 8e9567169d6df988e2caec6b7edad7 2a5158de4de60b6cc1e011ab0ccad7 f557974ec0730f58af9dcd03a892e3 8b470eebe951079ff69c1e6ec75acc 2c20dc240da2052d62c557f368bf94 07c2c92e5eaebe2b19b2ae1cbd2216 7d92432f1a1cef1a481385863d174a 46999086608471ef397ef3a3058dc5 6c1ccad647e21a44fff32fe76b8d8c3 a14315a815f4495367fc0229abfb04 7b6c43750752d1cbf7f800c2da9004 2c13f003aea0935c9a803a4df21dbb e4cd9fa6efbed2fd5d8e960cd870b4 4e63959b095cdad9efcd4a0f59f9d8 3b766060cc7dd3530cc7388568290 3385812480f79f73e5410df0691190 25767e95cc0a417344fbf608376281 c645e154f0157faa0064c06cf78608 6e17ee43f1711effb914daeacab1eb8 30daf540583c7c64cc1a804fb0043b 75ddccc9795ed4594393582a31840 d4d050741e1bad976c2d76c00b73b 87ab79735714e8a1760a4630f3b8c 7f71076efd7b1849888c34ea38d5c6 a151ba935c9525e49f5286f

{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.192, "satuan": "hPa"}, "suhu": {"nilai": 29.42499, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.62349, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.5995, "satuan": "cm"}, "waktu": "17/11/2023 02:01:26"}	29011bf88f62027017bb2eb14d5e76694b7aee640241c3ea186dcc99a8f8e9567169d6df988e2caec6b7edad72a5158de4de60b6cc1e011ab0ccad7f557974ec0730f58af9dcd03a892e38b470eebe951079ff69c1e6ec75acc2c20dc240da2052d62c557f368bf9407c2c92e5eaebe2b19b2ae1cbd22167d92432f1a1cef1a481385863d174a46999086608471ef397ef3a3058dc56c1ccad647e21a44fff32fe76b8d8c3a14315a815f4495367fc027fc1bb3a384db19cd4312ae09ac1f76c0e44a09c851c7500ff6ff79f53c1c16cb301ba7811724fbca6c314f935d7366f259d3aaae617bd6752a3eab66c089f2a22f4fc933ef51887ddb477b957f610bf16cc0f5b8813ebd0732425ed2ea0b10a465abaee54e495d8af02a4cfa09326cd2fed605e0b18199bf985281bda051bf569c9d3e9735bda4cd320e0bf557ecc4e02c45a2c8674d126f335565f2ecba788486b9fd9718f543766ade940af4b3694072f948e8248d8fb1b49bcc227f927ee8685c0e354fac5e97b1e4a00afa0cc8156ea644dac2e2ef75b34c80dfb20461a

2) Dengan Random String

Tabel 4.2 Pengujian Enkripsi Data Dengan Random String Tambahan

Plaintext	Ciphertext
SWCnMcVAJzjVT1Uj{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.159, "satuan": "hPa"}, "suhu": {"nilai": 29.45461, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.88422, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.8054, "satuan": "cm"}, "waktu": "17/11/2023 02:00:14"}	8b75117b5dd4fc2ac78c7da32bc7da4d59fd881b17cbbdcad6e126b44a7b319c560d5b664129cc39137a043e4ce2667a761c1bd919f71aa2996eea5bf318e807dbbc8f648d781bcf2c2ad609863c875cdd2b69a5e09bfc9ae19d5862d5c02664c37f8862e6b9e75c41fa8e7721a48235da737871de6edb8cd49298d94ce7ac1274c95df62cabc35252182ad8a35280f23d754beaf3db7bd600714c517f8e4eb6ad3fad081e6f2757d299e034e3074d414a8f7206ce580c6dd2235916a8c6464dbe76d6c1a65d57c53c9d32d081702de7ea69863a0326848522a36681c73135adb3d50238ac0385932a77189fc1b6657af1bc65cd54f780524345ea83d873fc0017788879451d77e94804838a5e4e48e1db912a4c0026d9fcc46af8f3f4ab4d3b48640e68379fc3eb6399e7562843e61dc6f7ecb6182e380c887353229acc1a64b9d9212853cc52988c8fe5d550f2317f5628ba7fd7fc13581d5b3ec8d719d9649531049af73d0fca58b3ed249de2854a144b72e1093b7b343e7022b3c475fca6adb80d231ef53ade0464982831b64bc435d1f8e6e20a51af71d493bc39695b8f
3VfENRtiKWIEVAO3{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.106, "satuan": "hPa"}, "suhu": {"nilai": 29.43684, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 51.3084, "satuan": "m"}}, "aj-sr04m": {"nilai":	3e97748fe421d5354d7be0479263ab956784714d3c92a712933365587a39370f2d864b24c3719f08159b283e4764ec2fcf8b07c8b781e37e166db96374394eed3bf235ee9a1ba044bddb6ac95f327987d13f0e1869bd0933474032c712fa1ffcabff80f01dae312b4c009d0ec5cf5ba783a7dd73e0c533008a9145ac882a21348a16f2445037268a509453e19dbd33b3a19b9df8d516e5a79877031c15c74017b95fdbed95dfce526a0c299de77d01afaaa4589aa8

602.6339, "satuan": "cm"}, "waktu": "17/11/2023 02:00:32"}	abc1e2f1db6fde7822bd00267416f340fe0ba69b132a7ba6fdcacf2967a0f21f641d3ee2f4e81ca0e7499c835764f20cc12efa4d990e622ef2dfddcc816a3cbc681166ab5ef159d591dccc0453defda8da5483ed67e42a9a3f4627eaa6969a28511358742f8a1b6d35a82ae93fbb4de8c8552d8c5603dbd658c99d1a87f68d0d28139e3f0d90107440982420136302afb37ae0086ef7d5c140df253f31ddc578003a1137b8ed706d09e00893d92f9247afc076da039a03366b04f7bee89fec5069f3797fa70eaf27289c251b9ab698419125f729939cde7e1bd7f7321f36297b5b5f676c4578af1985c3ad
rOAxUB4jH3K5IX0P{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.165, "satuan": "hPa"}, "suhu": {"nilai": 29.43684, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.83342, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.5995, "satuan": "cm"}, "waktu": "17/11/2023 02:00:50"}	e562768d38e1eb70f966e088d1a7090fcc7b758d852cd8df73445f4be4dd6738187c5176c92f835c1c71773fa9ff308ef1876560a47d2ee91eaec29c896f9eb9e583fc30f7627496d0d466f20704f31eb7d1c62f277211de80c8b2293a623d9cbbb8836f643684abee5c1f8da6879602d31e8145b216236b015b8241d49b4692296f6c05ccb983253068c5fefdc88d8cb7858429f64f50e35e62cfdb641b189219f96cadf609f726dc30562a81472f59ca0c113a3ef6afad314d9d68b9852c28d530ea98f1964477d203535bae3364a9b3ef0401f022aca23d62980ce48395173fd31016aef501c888bb3bfc22f5a5b76f3ee6090543cc8015743f3ac5d3306a4baa07edcf97396ca2fb9d8a260c72cf5a0db90a9d34a7cd3395e02de18a237204ca368d8e69ef77aff3b9dd4a45c86acfa5e0dc7efff5a711f73b0218b888dc6dd12f126a8002c0979cd98a8bbc067fe4554daacbbd86de8289ca2f3e2cc85a46fcc8894648753afb60ec080cfe5e749f34e12f2cb7ed1631a07224a545c8e41077297339d5de80d9579dc60822fce401e16f2fd1b5008a48b38f3d8891abe

gUut4dtNdcdwlmWg{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.132, "satuan": "hPa"}, "suhu": {"nilai": 29.42499, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 51.09703, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.7711, "satuan": "cm"}, "waktu": "17/11/2023 02:01:08"}	d75e9e7a55c3489ccf23fbf40b6753 55fb97c2193669898b8f8c11c58f44 9d81bc1323e4c768fcc4f66c34bd13 5075be7e11f278b24714ad3d62978 9dd740820a940ad297e007f3f52f36 8ce42ed0986e08a902c83d0da5bb30 17e3c7e22194229cc6e10ef4965385 b187dd623e6264fa232725f3e5ea4a d63e66db334d0630720ec7c3112a2 44cd0f4f7c09b090735cf467e45fa72 6a9c4fc6e4655ba792d959e91fdb9f 4627378f0c4d4ebb67458bfb24366e 10c633165851ab5ea5174c3b806a5e 0b2abc193a5e3c9ef22ec1f83b8171f 08bd5b6e044a6f94ecc6598a289c00 79bca4eb88da299ef384c6bb54faf7f a0e3db01787a973bcb91bd39807ae 14e361b7d6f78c8fc8ec340dc327ed 7c9bb7c7ccdb8759d213b292e6946 5eb3fd03101b776edb372ea162c995 2ffc24b12c1cae9a56d754c8a5767d adb8c1fea6e2cda3ec22c215a9be82 d24ad659e918cd00b8e7092e3a3c0c 5438a76cb99f56ca3adcae1d72f25b 17e25cba2f984ee973d1265d738690 cbb10ab3540e5c99712a1ac0fb3509 080810e541b6d30ec549a42df3371b cd6d24d96501005d6723924
VgAeA3niPrZCggQs{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.192, "satuan": "hPa"}, "suhu": {"nilai": 29.42499, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.62349, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.5995, "satuan": "cm"}, "waktu": "17/11/2023 02:01:26"}	4137b6c3c1ad87288b2bc1d3fbf5fe 00d4d5b88d69f95fabcd8984495512 427bfba3a81b4a07e4196eaa011e61 5cfd7d31d1b4bcc4edcc3ccee1c497 9579aa49203f554c9fcef518513431 e8ca16bf0397ff35520a05d44bcda7 5d30fafefc3032f5b5a04037cacd9c3 3c9f60ecf1ed5acfcfcfb68456aa91a3 65fab4463254ed5ac54603f6c3c154 c86db46006f1fcf790d3e01d05e69f5 f14b478d50a2673af078272fda6e5b d2f818cee9d3c373ff28767bd1aaada b8b993fc334470f207473089e4fea1 a55fe2f401ccedd8b18f969c1a82431 85cc075b76cb8a08de004c4c8b3cb0 a79ae02ed4dac3c323eb11f9ac7f18d

	e76f9a11e25ba6aab779feffe9ae64a 169d88b7e4df46465fe09fa40a816f5 c1c80e6792de54af65f63af6167b47 7553a4b659f2dcf915af57cba9a0bad 04807560187ab701c894a52d5bd47 5bab327afa0dc6124c5368765ade08 45eb2323d30565158cd604e18b1c2 a8e5d1fcfae6576466d17d63211cca 8978e9115cf5ff7d96bfafcde78a9f4 19c72690128d51050263d70b9d776 3a3c1608d59230a8ed4825a08faf1d e3cb32e5f144e5

4.2.6 Pengujian Perbandingan Hasil Enkripsi Dengan Tools Online

Tools online yang dilakukan pada pengujian di bawah ini menggunakan website http://aes.online-domain-tools.com/. Proses enkripsi di bawah dilakukan menggunakan kunci dan IV yang sama yaitu:

Kunci:

57cfde89a8614f3d1a3b556fab62a42684f5027d292b13f58266c5fce1e84538

IV: b4d5238a7aa4a6cbfdd75ee535eb9ed5

Tabel 4.3 Pengujian Perbandingan Hasil Enkripsi Dengan Tools Online

Plaintext	Hasil Enkripsi Pada Perangkat	Hasil Enkripsi Pada Tools Online
SWCnMcVAJzjVT1Uj{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.159, "satuan": "hPa"},	8b75117b5dd4fc2ac78c7da32bc7da4d59fd881b17cbbdcad6e126b44a7b319c560d5b664129cc39137a043e4ce2667a761c1bd919f71aa2996eea5bf318e807dbbc8f648d781bcf2c2ad609863c875cdd2b69a5e09bfc9ae19d5862d5c02664c37f8862e6b9e75c41fa8e7721a48235da737871de6edb8cd49298d94ce7ac1274c95df62cabc35252182ad8a35280f23d754beaf3db7bd600714c517f8e4eb6ad3fad081e6f2757d299e034e3074d414a8f7206ce580c6dd223591	8b75117b5dd4fc2ac78c7da32bc7da4d59fd881b17cbbdcad6e126b44a7b319c560d5b664129cc39137a043e4ce2667a761c1bd919f71aa2996eea5bf318e807dbbc8f648d781bcf2c2ad609863c875cdd2b69a5e09bfc9ae19d5862d5c02664c37f8862e6b9e75c41fa8e7721a48235da737871de6edb8cd49298d94ce7ac1274c95df62cabc35252182ad8a35280f23d754beaf3db7bd600714c517f8e4eb6ad3fad081e6f2757d299e034e3074d414a8f7206ce580c6dd223591

"suhu": {"nilai": 29.45461, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.88422, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.8054, "satuan": "cm"}, "waktu": "17/11/2023 02:00:14"}	6a8c6464dbe76d6c1a65d57c53c9d32d081702de7ea69863a0326848522a36681c73135adb3d50238ac0385932a77189fc1b6657af1bc65cd54f780524345ea83d873fc0017788879451d77e94804838a5e4e48e1db912a4c0026d9fcc46af8f3f4ab4d3b48640e68379fc3eb6399e7562843e61dc6f7ecb6182e380c887353229acc1a64b9d9212853cc52988c8fe5d550f2317f5628ba7fd7fc13581d5b3ec8d719d9649531049af73d0fca58b3ed249de2854a144b72e1093b7b343e7022b3c475fca6adb80d231ef53ade0464982831b64bc435d1f8e6e20a51af71d493bc39695b8f	6a8c6464dbe76d6c1a65d57c53c9d32d081702de7ea69863a0326848522a36681c73135adb3d50238ac0385932a77189fc1b6657af1bc65cd54f780524345ea83d873fc0017788879451d77e94804838a5e4e48e1db912a4c0026d9fcc46af8f3f4ab4d3b48640e68379fc3eb6399e7562843e61dc6f7ecb6182e380c887353229acc1a64b9d9212853cc52988c8fe5d550f2317f5628ba7fd7fc13581d5b3ec8d719d9649531049af73d0fca58b3ed249de2854a144b72e1093b7b343e7022b3c475fca6adb80d231ef53ade0464982831b64bc435d1f8e6e20a51af71d493bc39695b8f
3VfENRtiKWIEVAO3{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.106, "satuan": "hPa"}, "suhu": {"nilai": 29.43684, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 51.3084,	3e97748fe421d5354d7be0479263ab956784714d3c92a712933365587a39370f2d864b24c3719f08159b283e4764ec2fcf8b07c8b781e37e166db96374394eed3bf235ee9a1ba044bddb6ac95f327987d13f0e1869bd0933474032c712fa1ffcabff80f01dae312b4c009d0ec5cf5ba783a7dd73e0c533008a9145ac882a21348a16f2445037268a509453e19dbd33b3a19b9df8d516e5a79877031c15c74017b95fdbed95dfce526a0c299de77d01afaaa4589aa8abc1e2f1db6fde7822bd00267416f340fe0ba69b132a7ba6fdcacf2967a0f21f641d3ee2f4e81ca0e7499c835764f20cc12efa4d990e622ef2dfddcc816a3cbc681166ab5ef159d591dccc045	3e97748fe421d5354d7be0479263ab956784714d3c92a712933365587a39370f2d864b24c3719f08159b283e4764ec2fcf8b07c8b781e37e166db96374394eed3bf235ee9a1ba044bddb6ac95f327987d13f0e1869bd0933474032c712fa1ffcabff80f01dae312b4c009d0ec5cf5ba783a7dd73e0c533008a9145ac882a21348a16f2445037268a509453e19dbd33b3a19b9df8d516e5a79877031c15c74017b95fdbed95dfce526a0c299de77d01afaaa4589aa8abc1e2f1db6fde7822bd00267416f340fe0ba69b132a7ba6fdcacf2967a0f21f641d3ee2f4e81ca0e7499c835764f20cc12efa4d990e622ef2dfddcc816a3cbc681166ab5ef159d591dccc045

"satuan": "m"}}, "aj-sr04m": {"nilai": 602.6339, "satuan": "cm"}, "waktu": "17/11/2023 02:00:32"}	3defda8da5483ed67e42a9 a3f4627eaa6969a2851135 8742f8a1b6d35a82ae93fb b4de8c8552d8c5603dbd65 8c99d1a87f68d0d28139e3 f0d9010744098242013630 2afb37ae0086ef7d5c140df 253f31ddc578003a1137b8 ed706d09e00893d92f9247 afc076da039a03366b04f7 bee89fec5069f3797fa70ea f27289c251b9ab69841912 5f729939cde7e1bd7f7321f 36297b5b5f676c4578af19 85c3ad	3defda8da5483ed67e42a9 a3f4627eaa6969a2851135 8742f8a1b6d35a82ae93fb b4de8c8552d8c5603dbd65 8c99d1a87f68d0d28139e3 f0d9010744098242013630 2afb37ae0086ef7d5c140df 253f31ddc578003a1137b8 ed706d09e00893d92f9247 afc076da039a03366b04f7 bee89fec5069f3797fa70ea f27289c251b9ab69841912 5f729939cde7e1bd7f7321f 36297b5b5f676c4578af19 85c3ad
rOAxUB4jH3K5I X0P{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.165, "satuan": "hPa"}, "suhu": {"nilai": 29.43684, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.83342, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.5995, "satuan": "cm"},	e562768d38e1eb70f966e0 88d1a7090fcc7b758d852c d8df73445f4be4dd673818 7c5176c92f835c1c71773fa 9ff308ef1876560a47d2ee9 1eaec29c896f9eb9e583fc3 0f7627496d0d466f20704f 31eb7d1c62f277211de80c 8b2293a623d9cbbb8836f6 43684abee5c1f8da687960 2d31e8145b216236b015b 8241d49b4692296f6c05cc b983253068c5fefdc88d8c b7858429f64f50e35e62cfd b641b189219f96cadf609f7 26dc30562a81472f59ca0c 113a3ef6afad314d9d68b9 852c28d530ea98f1964477 d203535bae3364a9b3ef04 01f022aca23d62980ce483 95173fd31016aef501c888 bb3bfc22f5a5b76f3ee6090 543cc8015743f3ac5d3306 a4baa07edcf97396ca2fb9d 8a260c72cf5a0db90a9d34 a7cd3395e02de18a237204 ca368d8e69ef77aff3b9dd4 a45c86acfa5e0dc7effff5a7 11f73b0218b888dc6dd12f	e562768d38e1eb70f966e0 88d1a7090fcc7b758d852c d8df73445f4be4dd673818 7c5176c92f835c1c71773fa 9ff308ef1876560a47d2ee9 1eaec29c896f9eb9e583fc3 0f7627496d0d466f20704f 31eb7d1c62f277211de80c 8b2293a623d9cbbb8836f6 43684abee5c1f8da687960 2d31e8145b216236b015b 8241d49b4692296f6c05cc b983253068c5fefdc88d8c b7858429f64f50e35e62cfd b641b189219f96cadf609f7 26dc30562a81472f59ca0c 113a3ef6afad314d9d68b9 852c28d530ea98f1964477 d203535bae3364a9b3ef04 01f022aca23d62980ce483 95173fd31016aef501c888 bb3bfc22f5a5b76f3ee6090 543cc8015743f3ac5d3306 a4baa07edcf97396ca2fb9d 8a260c72cf5a0db90a9d34 a7cd3395e02de18a237204 ca368d8e69ef77aff3b9dd4 a45c86acfa5e0dc7effff5a7 11f73b0218b888dc6dd12f

"waktu": "17/11/2023 02:00:50"}	126a8002c0979cd98a8bbc067fe4554daacbbd86de8289ca2f3e2cc85a46fcc8894648753afb60ec080cfe5e749f34e12f2cb7ed1631a07224a545c8e41077297339d5de80d9579dc60822fce401e16f2fd1b5008a48b38f3d8891abe	126a8002c0979cd98a8bbc067fe4554daacbbd86de8289ca2f3e2cc85a46fcc8894648753afb60ec080cfe5e749f34e12f2cb7ed1631a07224a545c8e41077297339d5de80d9579dc60822fce401e16f2fd1b5008a48b38f3d8891abe
gUut4dtNdcdwlmWg{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.132, "satuan": "hPa"}, "suhu": {"nilai": 29.42499, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 51.09703, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.7711, "satuan": "cm"}, "waktu": "17/11/2023 02:01:08"}	d75e9e7a55c3489ccf23fbf40b675355fb97c2193669898b8f8c11c58f449d81bc1323e4c768fcc4f66c34bd135075be7e11f278b24714ad3d629789dd740820a940ad297e007f3f52f368ce42ed0986e08a902c83d0da5bb3017e3c7e22194229cc6e10ef4965385b187dd623e6264fa232725f3e5ea4ad63e66db334d0630720ec7c3112a244cd0f4f7c09b090735cf467e45fa726a9c4fc6e4655ba792d959e91fdb9f4627378f0c4d4ebb67458bfb24366e10c633165851ab5ea5174c3b806a5e0b2abc193a5e3c9ef22ec1f83b8171f08bd5b6e044a6f94ecc6598a289c0079bca4eb88da299ef384c6bb54faf7fa0e3db01787a973bcb91bd39807ae14e361b7d6f78c8fc8ec340dc327ed7c9bb7c7ccdb8759d213b292e69465eb3fd03101b776edb372ea162c9952ffc24b12c1cae9a56d754c8a5767dadb8c1fea6e2cda3ec22c215a9be82d24ad659e918cd00b8e7092e3a3c0c5438a76cb99f56ca3adcae1d72f25b17e25cba2f984ee973d1265d738690cbb10ab3540e5c99712a1ac0fb3509080	d75e9e7a55c3489ccf23fbf40b675355fb97c2193669898b8f8c11c58f449d81bc1323e4c768fcc4f66c34bd135075be7e11f278b24714ad3d629789dd740820a940ad297e007f3f52f368ce42ed0986e08a902c83d0da5bb3017e3c7e22194229cc6e10ef4965385b187dd623e6264fa232725f3e5ea4ad63e66db334d0630720ec7c3112a244cd0f4f7c09b090735cf467e45fa726a9c4fc6e4655ba792d959e91fdb9f4627378f0c4d4ebb67458bfb24366e10c633165851ab5ea5174c3b806a5e0b2abc193a5e3c9ef22ec1f83b8171f08bd5b6e044a6f94ecc6598a289c0079bca4eb88da299ef384c6bb54faf7fa0e3db01787a973bcb91bd39807ae14e361b7d6f78c8fc8ec340dc327ed7c9bb7c7ccdb8759d213b292e69465eb3fd03101b776edb372ea162c9952ffc24b12c1cae9a56d754c8a5767dadb8c1fea6e2cda3ec22c215a9be82d24ad659e918cd00b8e7092e3a3c0c5438a76cb99f56ca3adcae1d72f25b17e25cba2f984ee973d1265d738690cbb10ab3540e5c99712a1ac0fb3509080

	810e541b6d30ec549a42df3371bcd6d24d96501005d6723924	810e541b6d30ec549a42df3371bcd6d24d96501005d6723924
VgAeA3niPrZCggQs{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.192, "satuan": "hPa"}, "suhu": {"nilai": 29.42499, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.62349, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.5995, "satuan": "cm"}, "waktu": "17/11/2023 02:01:26"}	4137b6c3c1ad87288b2bc1d3fbf5fe00d4d5b88d69f95fabcd8984495512427bfba3a81b4a07e4196eaa011e615cfd7d31d1b4bcc4edcc3ccee1c4979579aa49203f554c9fcef518513431e8ca16bf0397ff35520a05d44bcda75d30fafefc3032f5b5a04037cacd9c33c9f60ecf1ed5acfcfcfb68456aa91a365fab4463254ed5ac54603f6c3c154c86db46006f1fcf790d3e01d05e69f5f14b478d50a2673af078272fda6e5bd2f818cee9d3c373ff28767bd1aaadab8b993fc334470f207473089e4fea1a55fe2f401ccedd8b18f969c1a8243185cc075b76cb8a08de004c4c8b3cb0a79ae02ed4dac3c323eb11f9ac7f18de76f9a11e25ba6aab779feffe9ae64a169d88b7e4df46465fe09fa40a816f5c1c80e6792de54af65f63af6167b477553a4b659f2dcf915af57cba9a0bad04807560187ab701c894a52d5bd475bab327afa0dc6124c5368765ade0845eb2323d30565158cd604e18b1c2a8e5d1fcfae6576466d17d63211cca8978e9115cf5ff7d96bfafcde78a9f419c72690128d51050263d70b9d7763a3c1608d59230a8ed4825a08faf1de3cb32e5f144e5	4137b6c3c1ad87288b2bc1d3fbf5fe00d4d5b88d69f95fabcd8984495512427bfba3a81b4a07e4196eaa011e615cfd7d31d1b4bcc4edcc3ccee1c4979579aa49203f554c9fcef518513431e8ca16bf0397ff35520a05d44bcda75d30fafefc3032f5b5a04037cacd9c33c9f60ecf1ed5acfcfcfb68456aa91a365fab4463254ed5ac54603f6c3c154c86db46006f1fcf790d3e01d05e69f5f14b478d50a2673af078272fda6e5bd2f818cee9d3c373ff28767bd1aaadab8b993fc334470f207473089e4fea1a55fe2f401ccedd8b18f969c1a8243185cc075b76cb8a08de004c4c8b3cb0a79ae02ed4dac3c323eb11f9ac7f18de76f9a11e25ba6aab779feffe9ae64a169d88b7e4df46465fe09fa40a816f5c1c80e6792de54af65f63af6167b477553a4b659f2dcf915af57cba9a0bad04807560187ab701c894a52d5bd475bab327afa0dc6124c5368765ade0845eb2323d30565158cd604e18b1c2a8e5d1fcfae6576466d17d63211cca8978e9115cf5ff7d96bfafcde78a9f419c72690128d51050263d70b9d7763a3c1608d59230a8ed4825a08faf1de3cb32e5f144e5

4.2.7 Pengujian Perbandingan Hasil Dekripsi Dengan Tools Online

Tools online yang dilakukan pada pengujian di bawah ini menggunakan website http://aes.online-domain-tools.com/. Proses dekripsi di bawah dilakukan menggunakan kunci dan IV yang sama yaitu:

Kunci: 57cfde89a8614f3d1a3b556fab62a42684f5027d292b13f58266c5fce1e84538

IV: b4d5238a7aa4a6cbfdd75ee535eb9ed5

Tabel 4.4 Pengujian Perbandingan Hasil Dekripsi Dengan Tools Online

Ciphertext	Hasil Dekripsi Pada Perangkat	Hasil Dekripsi Pada Tools Online
8b75117b5dd4fc2ac7 8c7da32bc7da4d59fd8 81b17cbbdcad6e126b 44a7b319c560d5b664 129cc39137a043e4ce 2667a761c1bd919f71 aa2996eea5bf318e807 dbbc8f648d781bcf2c2 ad609863c875cdd2b6 9a5e09bfc9ae19d5862 d5c02664c37f8862e6 b9e75c41fa8e7721a48 235da737871de6edb8 cd49298d94ce7ac127 4c95df62cabc3525218 2ad8a35280f23d754b eaf3db7bd600714c51 7f8e4eb6ad3fad081e6 f2757d299e034e3074 d414a8f7206ce580c6d d2235916a8c6464dbe 76d6c1a65d57c53c9d 32d081702de7ea6986 3a0326848522a36681 c73135adb3d50238ac 0385932a77189fc1b6 657af1bc65cd54f7805 24345ea83d873fc001 7788879451d77e9480 4838a5e4e48e1db912 a4c0026d9fcc46af8f3f 4ab4d3b48640e68379	SWCnMcVAJzjVT1Uj{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.159, "satuan": "hPa"}, "suhu": {"nilai": 29.45461, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.88422, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.8054, "satuan": "cm"}, "waktu": "17/11/2023 02:00:14"}	SWCnMcVAJzjVT1Uj{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.159, "satuan": "hPa"}, "suhu": {"nilai": 29.45461, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.88422, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.8054, "satuan": "cm"}, "waktu": "17/11/2023 02:00:14"}

fc3eb6399e7562843e61dc6f7ecb6182e380c887353229acc1a64b9d9212853cc52988c8fe5d550f2317f5628ba7fd7fc13581d5b3ec8d719d9649531049af73d0fca58b3ed249de2854a144b72e1093b7b343e7022b3c475fca6adb80d231ef53ade0464982831b64bc435d1f8e6e20a51af71d493bc39695b8f		
3e97748fe421d5354d7be0479263ab956784714d3c92a712933365587a39370f2d864b24c3719f08159b283e4764ec2fcf8b07c8b781e37e166db96374394eed3bf235ee9a1ba044bddb6ac95f327987d13f0e1869bd0933474032c712fa1ffcabff80f01dae312b4c009d0ec5cf5ba783a7dd73e0c533008a9145ac882a21348a16f2445037268a509453e19dbd33b3a19b9df8d516e5a79877031c15c74017b95fdbed95dfce526a0c299de77d01afaaa4589aa8abc1e2f1db6fde7822bd00267416f340fe0ba69b132a7ba6fdcacf2967a0f21f641d3ee2f4e81ca0e7499c835764f20cc12efa4d990e622ef2dfddcc816a3cbc681166ab5ef159d591dccc0453defda8da5483ed67e42a9a3f4627eaa6969a285113	3VfENRtiKWIEVAO3{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.106, "satuan": "hPa"}, "suhu": {"nilai": 29.43684, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 51.3084, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.6339, "satuan": "cm"}, "waktu": "17/11/2023 02:00:32"}	3VfENRtiKWIEVAO3{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.106, "satuan": "hPa"}, "suhu": {"nilai": 29.43684, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 51.3084, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.6339, "satuan": "cm"}, "waktu": "17/11/2023 02:00:32"}

58742f8a1b6d35a82ae93fbb4de8c8552d8c5603dbd658c99d1a87f68d0d28139e3f0d9010744098242013630 2afb37ae0086ef7d5c140df253f31ddc578003a1137b8ed706d09e00893d92f9247afc076da039a03366b04f7bee89fec5069f3797fa70eaf27289c251b9ab698419125f729939cde7e1bd7f7321f36297b5b5f676c4578af1985c3ad		
e562768d38e1eb70f966e088d1a7090fcc7b758d852cd8df73445f4be4dd6738187c5176c92f835c1c71773fa9ff308ef1876560a47d2ee91eaec29c896f9eb9e583fc30f7627496d0d466f20704f31eb7d1c62f277211de80c8b2293a623d9cbbb8836f643684abee5c1f8da6879602d31e8145b216236b015b8241d49b4692296f6c05ccb983253068c5fefdc88d8cb7858429f64f50e35e62cfdb641b189219f96cadf609f726dc30562a81472f59ca0c113a3ef6afad314d9d68b9852c28d530ea98f1964477d203535bae3364a9b3ef0401f022aca23d6298 0ce48395173fd31016aef501c888bb3bfc22f5a5b76f3ee6090543cc8015743f3ac5d3306a4baa07edcf97396ca2fb9d8a260c7	rOAxUB4jH3K5IX0P{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.165, "satuan": "hPa"}, "suhu": {"nilai": 29.43684, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.83342, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.5995, "satuan": "cm"}, "waktu": "17/11/2023 02:00:50"}	rOAxUB4jH3K5IX0P{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.165, "satuan": "hPa"}, "suhu": {"nilai": 29.43684, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.83342, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.5995, "satuan": "cm"}, "waktu": "17/11/2023 02:00:50"}

2cf5a0db90a9d34a7cd3395e02de18a237204ca368d8e69ef77aff3b9dd4a45c86acfa5e0dc7efff5a711f73b0218b888dc6dd12f126a8002c0979cd98a8bbc067fe4554daacbbd86de8289ca2f3e2cc85a46fcc8894648753afb60ec080cfe5e749f34e12f2cb7ed1631a07224a545c8e41077297339d5de80d9579dc60822fce401e16f2fd1b5008a48b38f3d8891abe		
d75e9e7a55c3489ccf23fbf40b675355fb97c2193669898b8f8c11c58f449d81bc1323e4c768fcc4f66c34bd135075be7e11f278b24714ad3d629789dd740820a940ad297e007f3f52f368ce42ed0986e08a902c83d0da5bb3017e3c7e22194229cc6e10ef4965385b187dd623e6264fa232725f3e5ea4ad63e66db334d0630720ec7c3112a244cd0f4f7c09b090735cf467e45fa726a9c4fc6e4655ba792d959e91fdb9f4627378f0c4d4ebb67458bfb24366e10c633165851ab5ea5174c3b806a5e0b2abc193a5e3c9ef22ec1f83b8171f08bd5b6e044a6f94ecc6598a289c0079bca4eb88da299ef384c6bb54faf7fa0e3db01787a973bcb91bd39807ae14e361b7d6	gUut4dtNdcdwlmWg{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.132, "satuan": "hPa"}, "suhu": {"nilai": 29.42499, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 51.09703, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.7711, "satuan": "cm"}, "waktu": "17/11/2023 02:01:08"}	gUut4dtNdcdwlmWg{"dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.132, "satuan": "hPa"}, "suhu": {"nilai": 29.42499, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 51.09703, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.7711, "satuan": "cm"}, "waktu": "17/11/2023 02:01:08"}

f78c8fc8ec340dc327e d7c9bb7c7ccdb8759d 213b292e69465eb3fd 03101b776edb372ea1 62c9952ffc24b12c1ca e9a56d754c8a5767da db8c1fea6e2cda3ec22 c215a9be82d24ad659 e918cd00b8e7092e3a 3c0c5438a76cb99f56c a3adcae1d72f25b17e2 5cba2f984ee973d1265 d738690cbb10ab3540 e5c99712a1ac0fb3509 080810e541b6d30ec5 49a42df3371bcd6d24 d96501005d6723924		
4137b6c3c1ad87288b 2bc1d3fbf5fe00d4d5b 88d69f95fabcd898449 5512427bfba3a81b4a 07e4196eaa011e615cf d7d31d1b4bcc4edcc3 ccee1c4979579aa4920 3f554c9fcef51851343 1e8ca16bf0397ff3552 0a05d44bcda75d30faf efc3032f5b5a04037ca cd9c33c9f60ecf1ed5a cfcfcfb68456aa91a36 5fab4463254ed5ac546 03f6c3c154c86db460 06f1fcf790d3e01d05e 69f5f14b478d50a2673 af078272fda6e5bd2f8 18cee9d3c373ff28767 bd1aaadab8b993fc334 470f207473089e4fea1 a55fe2f401ccedd8b18 f969c1a8243185cc075 b76cb8a08de004c4c8 b3cb0a79ae02ed4dac3 c323eb11f9ac7f18de7 6f9a11e25ba6aab779f	VgAeA3niPrZCggQs{"dht 11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.192, "satuan": "hPa"}, "suhu": {"nilai": 29.42499, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.62349, "satuan": "m"}}, "aj-sr04m": {"nilai": 602.5995, "satuan": "cm"}, "waktu": "17/11/2023 02:01:26"}	VgAeA3niPrZCggQs{" dht11": {"suhu": {"nilai": 29, "satuan": "C"}, "kelembapan": {"nilai": 90, "satuan": "%"}}, "ts300b": {"nilai": 3.3, "satuan": "NTU"}, "bmp180": {"tekanan udara": {"nilai": 1008.192, "satuan": "hPa"}, "suhu": {"nilai": 29.42499, "satuan": "C"}, "ketinggian dari permukaan laut": {"nilai": 50.62349, "satuan": "m"}}, "aj- sr04m": {"nilai": 602.5995, "satuan": "cm"}, "waktu": "17/11/2023 02:01:26"}

effe9ae64a169d88b7e 4df46465fe09fa40a81 6f5c1c80e6792de54af 65f63af6167b477553a 4b659f2dcf915af57cb a9a0bad04807560187 ab701c894a52d5bd47 5bab327afa0dc6124c5 368765ade0845eb232 3d30565158cd604e18 b1c2a8e5d1fcfae6576 466d17d63211cca897 8e9115cf5ff7d96bfafc de78a9f419c7269012 8d51050263d70b9d77 63a3c1608d59230a8e d4825a08faf1de3cb32 e5f144e5		

4.3 Waktu Proses

Tahap ini merupakan perhitungan waktu yang digunakan dalam proses pengiriman *LoRa*, enkripsi data sensor dan dekripsi ciphertext. Sistem dinilai dengan memperhatikan variasi panjang karakter data dalam satuan waktu detik.

4.3.1 Waktu Proses Pengiriman LoRa

Tabel 4.5 Waktu Proses Pengiriman LoRa

Percobaan Ke-	Jumlah Bit	Waktu Proses (detik)
1	3200	6,00067
2	3200	6,000686
3	3200	6,000679
4	3200	6,00068
5	3200	6,000699
6	3200	6,000682
7	3200	6,000679
8	3200	6,000681
9	3200	6,00068
10	3200	6,000671
11	3200	6,000726
12	3200	6,000734

13	3200	6,000692
14	3200	6,000707
15	3200	6,000696
16	3200	6,000705
17	3200	6,000743
18	3200	6,000687
19	3200	6,00069
20	3200	6,000731
21	3200	6,000691
22	3200	6,000706
23	3200	6,000731
24	3200	6,000687
25	3200	6,00069
Rata – Rata	3200	6,00069692

4.3.2 Waktu Proses Enkripsi

Tabel 4.6 Waktu Proses Enkripsi

Percobaan Ke-	Jumlah Karakter	Waktu Proses (detik)
1	397	0,001213
2	397	0,00121
3	398	0,001202
4	398	0,001203
5	396	0,001278
6	398	0,001267
7	397	0,001212
8	398	0,001198
9	397	0,001207
10	398	0,001198
11	398	0,001217
12	398	0,00123
13	398	0,001218
14	396	0,001199
15	398	0,00121
16	398	0,001198
17	397	0,001216
18	398	0,001251
19	398	0,001223

20	398	0,001196
21	398	0,001202
22	398	0,001195
23	398	0,001209
24	398	0,001247
25	397	0,001219
Rata - Rata	397,6	0,00121672

4.3.3 Waktu Proses Dekripsi

Tabel 4.7 Waktu Proses Dekripsi

Percobaan Ke-	Jumlah Bit	Waktu Proses (detik)
1	3200	0,001452
2	3200	0,001498
3	3200	0,001509
4	3200	0,001489
5	3200	0,00149
6	3200	0,0015
7	3200	0,001494
8	3200	0,001506
9	3200	0,00149
10	3200	0,001495
11	3200	0,001495
12	3200	0,001511
13	3200	0,001487
14	3200	0,001504
15	3200	0,001483
16	3200	0,001511
17	3200	0,001494
18	3200	0,001515
19	3200	0,00149
20	3200	0,001502
21	3200	0,001491
22	3200	0,001507
23	3200	0,001488
24	3200	0,001499
25	3200	0,001482
Rata - Rata	3200	0,00149528

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berikut beberapa hasil yang dapat disimpulkan dari penelitian ini:

1) Penerapan *Hybrid Cryptosystem* menggunakan algoritma *Elliptic Curve Cryptography (ECC)* dan algoritma *Advanced Encryption Standard (AES)* dan berhasil mengamankan data yang dikirim melalui komunikasi jarak jauh *LoRa*.
2) Proses dekripsi dari *ciphertext* data yang sama seperti *plaintext*.
3) Mikrokontroller ESP32 mampu melakukan proses dari komputasi shared secret, proses enkripsi dan proses dekripsi.
4) Alat dapat bekerja sesuai dengan tujuan dari penelitian ini.

5.2 Saran

1) Dalam penelitian berikutnya, diharapkan sistem dapat dikembangkan untuk protokol komunikasi lain seperti Bluetooth, Ethernet, MQTT dan sebagainya.
2) Pada penelitian selanjutnya diharapkan dapat mengembangkan pengiriman data pada *LoRa* dengan ukuran yang lebih besar seperti untuk data file, audio, atau gambar.

DAFTAR PUSTAKA

Abroshan, H. (2021). A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 12, Issue 6). www.ijacsa.thesai.org

Al-Mashhadani, M., & Shujaa, M. (2022). IoT Security Using AES Encryption Technology based ESP32 Platform. *International Arab Journal of Information Technology*, *19*(2), 214–223. https://doi.org/10.34028/iajit/19/2/8

Azhari, M., Perwitosari, J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(1), 2809–476. https://doi.org/10.47709/jpsk.v2i1.1390

Chahin, N., & Mansour, A. (2023). Improving the IoT and Cloud Computing integration using Hybrid Encryption. *DESIGN, CONSTRUCTION, MAINTENANCE*, *3*, 1–6. https://doi.org/10.37394/232022.2023.3.1

Fadhil, M. S., Farhan, A. K., & Fadhil, M. N. (2021). A lightweight aes algorithm implementation for secure iot environment. *Iraqi Journal of Science*, *62*(8), 2759–2770. https://doi.org/10.24996/ijs.2021.62.8.29

Nugroho, Y., & Painem, P. (2022). IMPLEMENTASI ALGORITMA ELLIPTIC CURVE CRYPTOGRAPHY (ECC) UNTUK PENGAMANAN FILE BERBASIS WEB. In *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia*.

Omid Mahdi Ebadati, E., Eshghi, F., & Zamani, A. (2020). A hybrid encryption algorithm for security enhancement of wireless sensor networks: A supervisory approach to pipelines. *CMES - Computer Modeling in Engineering and Sciences*, *122*(1), 323–349. https://doi.org/10.32604/cmes.2020.08079

Potensi Utama Jl KLYos, U. (2019a). RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE

CHIPER DAN RSA BERBASIS ANDROID Yusfrizal 1). *Jurnal Teknik Informatika Kaputama (JTIK)*, *3*(2).

Potensi Utama Jl KLYos, U. (2019b). RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID Yusfrizal 1). *Jurnal Teknik Informatika Kaputama (JTIK)*, *3*(2).

Ramadani, S., & Sauda, S. (2020). Penerapan Algoritma AES dan DSA Menggunakan Hybrid Cryptosystem untuk Keamanan Data. *Jurnal Riset Komputer)*, *7*(4), 2407–389. https://doi.org/10.30865/jurikom.v7i4.2055

Yang, H. (2022). Application of Hybrid Encryption Algorithm in Hardware Encryption Interface Card. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/7794209

Zaki Fadilla Rangkuti, A., Fahmi, H., & Pelita Nusantara, S. (2020). Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5. *Jurnal Nasional Komputasi Dan Teknologi Informasi*, *3*(2).