IMPLEMENTASI ALGORITMA VIGENERE CIPHER PADA SISTEM TRANSMISI PESAN DARURAT PASCA-BENCANA MENGGUNAKAN LORA

MUHAMMAD FARHAN MUBARAK
H1051211103

SKRIPSI

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2026

IMPLEMENTASI ALGORITMA VIGENERE CIPHER PADA SISTEM TRANSMISI PESAN DARURAT PASCA-BENCANA MENGGUNAKAN LORA

MUHAMMAD FARHAN MUBARAK
H1051211103

Skripsi
Sebagai salah satu syarat untuk memperoleh gelar
Sarjana Sains pada Program Studi Rekayasa Sistem Komputer

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2026

LEMBAR PENGESAHAN

Judul Tugas Akhir	: Implementasi Algoritma *Vigenere Cipher* Pada Sistem Transmisi Pesan Darurat Pasca-Bencana Menggunakan LoRa
Nama Mahasiswa	: Muhammad Farhan Mubarak
NIM	: H1051211103
Jurusan/Program Studi	: Rekayasa Sistem Komputer
Tanggal Lulus	: 30 Juli 2026
SK Pembimbing	: 3942/UN22.8/TD.06/2025/17 November 2025
SK Penguji	: 5017/DST/UN22.8/DT.00.09/2026/29 Juli 2026

Dosen Pembimbing

Pembimbing I	Pembimbing II
Hirzen Hasfani, S.Kom., M.Cs.	Hafiz Muhardi, S.T., M.Kom.
NIP. 199305032022031003	NIP. 199007232023211017

Dosen Penguji

Ketua Penguji	Anggota Penguji
Kasliono, S.Mat., M.Cs.	Uray Ristian, S.Kom., M.Kom.
NIP. 199306202022031005	NIP. 199012012019031017

Pimpinan Sidang (merangkap anggota penguji)	Sekretaris Sidang (merangkap anggota penguji)
Hirzen Hasfani, S.Kom., M.Cs.	Hafiz Muhardi, S.T., M.Kom.
NIP. 199305032022031003	NIP. 199007232023211017

Mengesahkan
Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Tanjungpura

Prof. Dr. Gusrizal, S.Si., M.Si.
NIP. 197108022000031001

PERNYATAAN INTEGRITAS AKADEMIK

Saya yang bertanda tangan di bawah ini:

Nama	**: Muhammad Farhan Mubarak**
NIM	**: H1051211103**
Program Studi/ Jurusan	**: Rekayasa Sistem Komputer**
Fakultas	**: Matematika dan Ilmu Pengetahuan Alam**

dengan ini menyatakan bahwa dokumen ilmiah Tugas Akhir yang disajikan ini tidak mengandung unsur pelanggaran integritas akademik sesuai Peraturan Menteri Pendidikan, Kebudayaan, Riset, Dan Teknologi Republik Indonesia Nomor 39 Tahun 2021. Apabila di kemudian hari dokumen ilmiah Tugas Akhir ini mengandung unsur pelanggaran integritas akademik sesuai ketentuan perundangan tersebut, maka saya bersedia menerima sanksi akademik dan/atau sanksi hukum yang berlaku.

Demikian pernyatan ini untuk digunakan sebagaimana mestinya.

Pontianak,



Muhammad Farhan Mubarak
NIM. H1051211103

Implementasi Algoritma *Vigenere Cipher* Pada Sistem Transmisi Pesan Darurat Pasca-Bencana Menggunakan LoRa

Abstrak

Indonesia merupakan negara dengan tingkat kerawanan bencana yang tinggi sehingga diperlukan sistem komunikasi yang tetap dapat berfungsi ketika jaringan seluler dan internet mengalami gangguan. LoRa (*Long Range*) dapat dimanfaatkan sebagai media komunikasi alternatif karena mampu melakukan transmisi data jarak jauh tanpa bergantung pada jaringan. Namun, komunikasi LoRa belum menyediakan mekanisme pengamanan pesan sehingga berpotensi mengalami penyadapan oleh pihak yang tidak berwenang. Penelitian ini bertujuan menganalisis penerapan algoritma *Vigenère Cipher* terhadap serangan *sniffing* dan *brute force*, serta menganalisis pengaruhnya terhadap penggunaan memori dan waktu pemrosesan pada sistem transmisi pesan darurat berbasis LoRa. Sistem diimplementasikan menggunakan dua buah ESP32 dan modul LoRa SX1278. Pengujian dilakukan melalui simulasi *sniffing*, simulasi *brute force* dengan variasi panjang kunci 2 hingga 6 karakter, serta pengukuran waktu enkripsi, waktu dekripsi, dan penggunaan memori pada variasi panjang pesan 69 hingga 95 karakter dengan jarak transmisi 20 hingga 100 meter. Hasil pengujian menunjukkan bahwa pada proses *sniffing* penyerang hanya memperoleh ciphertext sehingga isi pesan tidak dapat dibaca tanpa mengetahui kunci. Pada pengujian *brute force*, seluruh kunci berhasil ditemukan, namun waktu pencarian meningkat dari 0,00277–0,01237 detik pada kunci 2 karakter menjadi 82,94911–1574,58623 detik pada kunci 6 karakter. Selain itu, jarak transmisi tidak berpengaruh signifikan terhadap waktu pemrosesan maupun penggunaan memori. Waktu enkripsi berada pada rentang 0,2376–0,2839 ms, waktu dekripsi 0,2133–0,2462 ms, dan penggunaan memori 96–112 byte. Hasil penelitian menunjukkan bahwa algoritma Vigenère Cipher mampu menjaga kerahasiaan pesan terhadap penyadapan dengan kebutuhan sumber daya yang rendah pada ESP32.

Kata Kunci: LoRa, *Vigenère Cipher*, pesan darurat, *Brute Force*, *Sniffing*, ESP32, Waktu Pemrosesan, Penggunaan Memori.

Implementation of the Vigenère Cipher Algorithm in Post-Disaster Emergency Message Transmission Systems Using LoRa

Abstract

Indonesia is a country with a high risk of natural disasters, making it essential to establish a communication system that remains operational when cellular and internet networks are disrupted. LoRa (Long Range) can be utilized as an alternative communication medium because it enables long-distance data transmission without relying on network infrastructure. However, LoRa communication does not provide a built-in message security mechanism, making transmitted data vulnerable to unauthorized interception. This study aims to analyze the implementation of the Vigenère Cipher algorithm against sniffing and brute-force attacks, as well as its impact on memory usage and processing time in a LoRa-based emergency message transmission system. The system was implemented using two ESP32 microcontrollers and LoRa SX1278 modules. The evaluation consisted of sniffing simulations, brute-force simulations with key lengths ranging from 2 to 6 characters, and measurements of encryption time, decryption time, and memory usage using message lengths of 69 to 95 characters over transmission distances of 20 to 100 meters. The results show that, during the sniffing simulation, an attacker could only obtain ciphertext, making the message unreadable without the encryption key. In the brute-force test, all keys were successfully recovered; however, the required search time increased from 0.00277–0.01237 seconds for 2-character keys to 82.94911–1574.58623 seconds for 6-character keys. Furthermore, the transmission distance had no significant effect on processing time or memory usage. The encryption time ranged from 0.2376 to 0.2839 ms, the decryption time ranged from 0.2133 to 0.2462 ms, and memory usage ranged from 96 to 112 bytes. These results indicate that the Vigenère Cipher algorithm is capable of maintaining message confidentiality against interception while requiring relatively low computational resources on the ESP32.

Keywords**:** *LoRa, Vigenère Cipher, Emergency Messages, Brute Force, Sniffing, ESP32, Processing Time, Memory Usage.*

PRAKATA

Segala puji dan syukur panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul **"Implementasi Algoritma Vigenere Cipher pada Sistem Transmisi Pesan Darurat Pasca-Bencana Menggunakan LoRa"** Tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom.) pada Jurusan Rekayasa Sistem Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Tanjungpura Pontianak.

Semua hasil yang diperoleh ini tidak lepas dari segala dukungan dan bantuan dari berbagai pihak yang terus mendorong penulis untuk menyelesaikan tugas akhir ini dengan baik. Sebagai penghargaan, izinkanlah penulis mengucapkan rasa terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. Gusrizal, S.Si., M.Si., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.
2. Ibu Rahmi Hidayati, S.Kom., M.Cs., selaku Ketua Jurusan Rekayasa Sistem Komputer FMIPA Universitas Tanjungpura Pontianak.
3. Bapak Hirzen Hasfani, S.Kom., M.Cs., sebagai dosen Pembimbing Pertama sekaligus sebagai dosen Pembimbing Akademik (PA) yang telah memberikan masukan serta meluangkan waktu dan pikiran yang memberikan dorongan dalam bimbingan penulisan skripsi.
4. Bapak Hafiz Muhardi, S.T., M.Kom., sebagai dosen Pembimbing Kedua yang telah memberikan masukan serta meluangkan waktu dan pikiran yang memberikan dorongan dalam bimbingan penulisan skripsi.
5. Bapak Kasliono, S.Mat., M.Cs., selaku dosen Penguji Pertama, yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.
6. Bapak Uray Ristian, S.Kom., M.Kom., selaku dosen Penguji Kedua, yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.

7. **Seluruh dosen Program Studi Rekayasa Sistem Komputer yang telah memberikan ilmu, wawasan dan pengalaman selama perkuliahan sehingga menjadi bekal dalam penyusunan skripsi ini.**
8. **Seluruh staff Program Studi Rekayasa Sistem Komputer yang telah memberikan bantuan, pelayanan, serta dukungan administrasi selama proses perkuliahan hingga penyusunan skripsi ini.**
9. **Kepada orang tua yang selalu memberikan dukungan, doa, motivasi, dan kasih sayang tanpa henti sepanjang perjalanan penulisan tugas akhir ini.**
10. Penulis mengucapkan terima kasih kepada Agustin Widianingsih atas doa, dukungan, motivasi, perhatian, serta kesabaran yang telah diberikan selama proses penyusunan skripsi ini. Semangat dan kehadirannya menjadi penyemangat dalam menghadapi berbagai tantangan selama penelitian hingga skripsi ini dapat diselesaikan.
11. Para rekan-rekan seperjuangan mahasiswa khususnya Sistem Komputer 2021 (NeMoTic) yang telah memberikan semangat dan dukungan dalam menjalani proses perkuliahan dan penulisan tugas akhir ini.
12. Semua pihak yang terlibat langsung maupun yang tidak langsung dalam penulisan tugas akhir ini.

Pontianak,



Muhammad Farhan Mubarak

DAFTAR ISI

PERNYATAAN INTEGRITAS AKADEMIK ..... **iii**
Abstrak ..... **iv**
Abstract ..... **v**
PRAKATA ..... **vi**
DAFTAR ISI ..... **viii**
DAFTAR GAMBAR ..... **x**
DAFTAR TABEL ..... **xi**
DAFTAR KODE PROGRAM ..... **xii**
BAB 1 PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 3
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 3
1.6 Sistematika Penulisan 4
BAB 2 LANDASAN TEORI **6**
2.1 Perbandingan dengan penelitian terdahulu 6
2.2 *Internet Of Things* 8
2.3 Kriptografi 8
2.4 Algoritma Kriptografi *Vigenere Cipher* 8
2.5 NodeMCU ESP32 9
2.6 LoRa SX1278 10
2.7 Arduino IDE 10
2.8 *Sniffing* 11
2.9 *Brute Force* 11
2.10 Waktu Pemrosesan 12
2.11 *Cryptool* 12
2.12 Visual Studio Code 12
BAB 3 METODE PENELITIAN **14**
3.1 Studi Literatur 15

3.2 Analisis Kebutuhan 15
3.2.1 Kebutuhan Perangkat Keras 15
3.2.2 Kebutuhan Perangkat Lunak 15
3.3 Perancangan Sistem 15
3.3.1 Perancangan Perangkat Keras 15
3.3.2 Perancangan Perangkat Lunak 16
3.4 Implementasi Sistem 16
3.5 Pengujian Sistem 16
3.6 Kesimpulan dan Saran 17
BAB 4 PERANCANGAN 18
4.1 Deskripsi Sistem 18
4.2 Perancangan Arsitektur Sistem 18
4.3 Perancangan Perangkat Keras 19
4.4 Perancangan Perangkat Lunak 21
4.5 Perancangan Implementasi Algoritma Vigenere Cipher 22
4.6 Perancangan Pengujian dengan *Brute Force dan Sniffing* 26
4.7 Perancangan Pengujian Waktu Pemrosesan dan Penggunaan Memori 27
4.8 Perancangan Pengujian Fungsional Sistem 29
BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN 31
5.1 Implementasi Sistem 31
5.2 Implementasi Perangkat Keras 31
5.3 Implementasi Perangkat Lunak 32
5.4 Implementasi Algoritma Vigenere Cipher 33
5.5 Pengujian dengan Serangan Brute Force dan Sniffing 37
5.6 Pengujian Waktu Pemrosesan dan Penggunaan Memori 45
5.7 Pengujian Fungsional Sistem 50
5.8 Pembahasan 52
BAB 6 PENUTUP 55
6.1 Kesimpulan 55
6.2 Saran 56
DAFTAR PUSTAKA 57
LAMPIRAN 59

DAFTAR GAMBAR

Gambar 2. 1 NodeMCU ESP32 9
Gambar 2. 2 LoRa SX1278 10
Gambar 2. 3 Arduino IDE 11
Gambar 3. 1 Diagram Alir Penelitian 14
Gambar 4. 1 Perancangan Arsitektur Sistem 19
Gambar 4. 2 Perancangan Keseluruhan Perangkat Keras 20
Gambar 4. 3 Diagram Alir Kerja Sistem 21
Gambar 4. 4 Diagram Alir Proses Enkripsi 22
Gambar 4. 5 Diagram Alir Proses Dekripsi 24
Gambar 5. 1 Implementasi Perangkat Keras 32
Gambar 5. 3 Ketika Mengirim Pesan 33
Gambar 5. 2 Ketika Menerima Pesan 33
Gambar 5. 4 Grafik Pengujian Brute Force 45
Gambar 5. 5 Grafik Pengujian Waktu Pemrosesan 49
Gambar 5. 6 Grafik Pengujian Penggunaan Memori 50

DAFTAR TABEL

Tabel 2. 1 Perbandingan dengan Penelitian Terdahulu 6
Tabel 4. 1. Penggunaan Pin ESP32 dengan Modul LoRa SX1278.....20
Tabel 4. 2 Langkah Pengujian terhadap Serangan Brute Force dan Sniffing.....26
Tabel 5. 1 Hasil Pengujian Metode *Sniffing* 38
Tabel 5. 2 Hasil Pengujian Metode *Brute Force* 39
Tabel 5. 3 Hasil Pengujian Waktu Pemrosesan dan Penggunaan Memori pada Panjang Pesan 69 karakter..... 46
Tabel 5. 4 Hasil Pengujian Waktu Pemrosesan dan Penggunaan Memori pada Panjang Pesan 79 Karakter..... 46
Tabel 5. 5 Hasil Pengujian Waktu Pemrosesan dan Penggunaan Memori pada Panjang Pesan 86 Karakter..... 47
Tabel 5. 6 Hasil Pengujian Waktu Pemrosesan dan Penggunaan Memori pada Panjang Pesan 91 Karakter..... 48
Tabel 5. 7 Hasil Pengujian Waktu Pemrosesan dan Penggunaan Memori pada Panjang Pesan 95 Karakter..... 48
Tabel 5. 8 Hasil Pengujian Fungsional Sistem 51

DAFTAR KODE PROGRAM

Kode Program 5. 1 Proses Enkripsi Vigenere Cipher 34
Kode Program 5. 2 Proses Dekripsi Vigenere Cipher.....35
Kode Program 5. 3 Dekripsi Vigenere Cipher 36
Kode Program 5. 4 Pembentukan Kandidat Kunci.....36
Kode Program 5. 5 Validasi Plaintext Kandidat 36
Kode Program 5. 6 Pengukuran Waktu Brute Force.....37

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Negara Indonesia merupakan negara kepulauan terbesar di dunia yang memiliki 17.499 pulau dari Sabang hingga Merauke. Sebanyak 28 wilayah di Negara Kesatuan Republik Indonesia dikategorikan sebagai wilayah rawan bencana (Candra et al., 2021). Setiap tahunnya, berbagai wilayah di Indonesia mengalami bencana yang tidak hanya menimbulkan kerugian material, tetapi juga mengancam keselamatan jiwa masyarakat. Pada kondisi pascabencana, infrastruktur komunikasi seperti jaringan internet dan sinyal seluler sering mengalami gangguan atau bahkan tidak dapat digunakan sehingga menghambat proses koordinasi, penyampaian informasi, dan penyaluran bantuan. Oleh karena itu, diperlukan sistem komunikasi yang mampu beroperasi tanpa bergantung pada jaringan.

LoRa (Long Range) merupakan teknologi komunikasi nirkabel jarak jauh yang menggunakan teknik modulasi *Chirp Spread Spectrum (CSS)* sehingga mampu melakukan transmisi data pada jarak yang jauh dengan konsumsi daya yang rendah (Darmawan et al., 2024). Pada penelitian ini, komunikasi LoRa dioperasikan pada frekuensi 433 Mhz untuk mengirimkan pesan darurat antar mikrokontroler. Transmisi data melalui LoRa dikirim menggunakan gelombang radio. Hal ini menyebabkan pihak yang tidak berwenang masih berpotensi menangkap paket data apabila menggunakan perangkat LoRa yang dikonfigurasi pada frekuensi yang sama. Akibatnya, pesan yang dikirim dapat disadap dan diperoleh dalam bentuk ciphertext.

Apabila penyerang berhasil memperoleh *ciphertext*, maka *ciphertext* yang dikirimkan dapat diperoleh tanpa harus mengakses perangkat pengirim maupun penerima secara langsung. *Ciphertext* hasil penyadapan tersebut berpotensi dianalisis lebih lanjut melalui metode serangan, salah satunya menggunakan metode *brute force* dengan mencoba berbagai kemungkinan kunci hingga menemukan *plaintext* dan kunci yang sesuai. Risiko penyadapan menjadi hal yang

perlu diperhatikan, terutama ketika sistem digunakan untuk mengirim informasi darurat yang bersifat penting, seperti lokasi korban, kondisi korban, dan jenis bantuan yang dibutuhkan. Oleh karena itu, diperlukan mekanisme pengamanan yang mampu melindungi kerahasiaan pesan dari risiko penyadapan *(sniffing)* dan upaya pemecahan kunci selama proses transmisi berlangsung.

Salah satu algoritma kriptografi yang memiliki proses komputasi ringan dan sesuai untuk diterapkan pada perangkat mikrokontroler adalah *Vigenere Cipher. Vigenere Cipher* merupakan algoritma kriptografi yang bekerja dengan memanfaatkan pergeseran karakter berdasarkan kunci menggunakan tabel *Vigenere* sehingga pesan asli (plaintext) diubah menjadi pesan terenkripsi *(*ciphertext*)* yang tidak dapat dipahami tanpa mengetahui kunci yang digunakan (Rivaldi et al., 2023). Dengan menerapkan algoritma *Vigenere Cipher* sebelum proses pengiriman melalui LoRa, informasi darurat yang dikirimkan tetap terlindungi meskipun berhasil ditangkap oleh pihak yang tidak berwenang.

Berdasarkan permasalahan tersebut, penelitian ini mengimplementasikan algoritma *Vigenere Cipher* pada sistem transmisi pesan darurat pascabencana menggunakan LoRa. Penelitian ini bertujuan untuk menganalisis keamanan algoritma *Vigenere Cipher* terhadap serangan *brute force* serta mengukur performanya dari sisi waktu pemrosesan dan penggunaan memori pada mikrokontroler, sehingga dapat diketahui kelayakannya sebagai mekanisme pengamanan komunikasi pesan darurat berbasis LoRa.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana penerapan algoritma *Vigenere Cipher* terhadap serangan *brute force* dan *sniffing* pada sistem komunikasi antar mikrokontroler berbasis LoRa?
2. Bagaimana pengaruh penerapan algoritma *Vigenere Cipher* terhadap penggunaan memori dan waktu pemrosesan mikrokontroler pada sistem transmisi pesan darurat berbasis LoRa?

1.3 Batasan Masalah

Batasan masalah penelitian ini adalah sebagai berikut:

1. Sistem dibangun menggunakan dua perangkat mikrokontroler yang saling berkomunikasi.
2. LoRA SX1278 digunakan sebagai transmisi pesan darurat.
3. Pesan darurat yang dikirim berupa teks, seperti informasi korban, lokasi atau peringatan darurat.
4. Algoritma enkripsi yang digunakan adalah *Vigenere Cipher*, diterapkan untuk mengamankan pesan sebelum dikirim dan didekripsi pada penerima pesan.
5. Pengujian jarak transmisi data dilakukan dijarak 20,40,60,80 dan 100 meter.
6. Pengujian sistem dilakukan dalam lingkungan terbatas untuk mensimulasikan kondisi pasca-bencana.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menganalisis algoritma *Vigenere Cipher* terhadap serangan *brute force* dan *sniffing* dalam komunikasi antar mikrokontroler.
2. Mengukur dan menganalisis performa algoritma Vigenere Cipher dalam hal penggunaan memori dan waktu pemrosesan saat diimplementasikan pada mikrokontroler.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah menambah pemahaman mengenai penerapan algoritma *Vigenere Cipher* pada sistem komunikasi berbasis LoRa, khususnya dalam mengukur performa penggunaan memori, waktu pemrosesan dan ketahanan sistem terhadap serangan *brute force*. Penelitian ini memberikan komunikasi darurat yang tetap berfungsi tanpa jaringan internet dan mendukung koordinasi pasca-bencana dengan menjaga kerahasiaan dari pesan darurat.

1.6 Sistematika Penulisan

Penulisan skripsi ini dibagi menjadi 6 bab agar permasalahan dapat dijelaskan dan diuraikan untuk menyelesaikan penelitian ini. Adapun sistematika penulisan tugas akhir ini terdiri dari:

BAB 1 PENDAHULUAN

Bab pendahuluan berisi latar belakang untuk menjelaskan tentang permasalahan keamanan pada jalur komunikasi perangkat LoRa dan kenapa penelitian ini dilakukan, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab landasan teori membahas teori-teori dan penelitian terdahulu yang digunakan sebagai pendukung dalam tugas akhir. Materi yang dibahas pada bab ini berupa NodeMCU ESP32, Algoritma Kriptografi *Vigenere Cipher*, Arduino IDE.

BAB 3 METODE PENELITIAN

Bab metode penelitian adalah prosedur atau cara-cara yang dilakukan untuk mengumpulkan dan menganalisis data serta menjawab pertanyaan atau hipotesis yang telah ditetapkan dalam penelitian. Adapun isi dari metode penelitian yaitu diagram alir, studi literatur, analisis kebutuhan, perancangan sistem, implementasi sistem, pengujian sistem, data hasil pengujian, kesimpulan dan saran.

BAB 4 PERANCANGAN

Bab perancangan berisi secara rinci tentang perancangan dan tahapan dalam pelaksanaan penelitian. Pada bab ini secara umum meliputi perancangan pada perangkat keras dan perangkat lunak. Pada perancangan perangkat keras terdiri dari perancangan sistem transmisi pesan darurat menggunakan NodeMCU ESP32 dan modul LoRa SX1278, dan perancangan keseluruhan perangkat keras. Sedangkan pada perancangan perangkat lunak meliputi perancangan sistem komunikasi dan perancangan metode algoritma kriptografi *Vigenere Cipher* pada sistem transmisi pesan darurat.

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Bab implementasi, pengujian, dan pembahasan membahas mengenai analisis

dan implementasi sistem yang telah dirancang pada tahap sebelumnya. Tahapan ini yaitu implementasi perangkat keras, implementasi perangkat lunak, pengujian, dan pembahasan.

BAB 6 PENUTUP

Bab penutup merupakan bab yang membahas tentang kesimpulan dari penelitian yang telah dilakukan dan saran terhadap masalah yang belum terselesaikan untuk dapat diperbaiki dan dikembangkan pada penelitian berikutnya.