IMPLEMENTASI KRIPTOGRAFI *ONE-TIME PAD* UNTUK KEAMANAN PENGIRIMAN DATA PADA SISTEM MONITORING PENGISIAN TOKEN LISTRIK PRABAYAR

WAHDIYAH
H1051201055

SKRIPSI

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

IMPLEMENTASI KRIPTOGRAFI *ONE-TIME PAD* UNTUK KEAMANAN PENGIRIMAN DATA PADA SISTEM MONITORING PENGISIAN TOKEN LISTRIK PRABAYAR

WAHDIYAH
H1051201055

Skripsi
Sebagai salah satu syarat untuk memperoleh gelar
Sarjana Komputer 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 Kriptografi *One-Time Pad* Untuk Keamanan Pengiriman Data Pada Sistem Monitoring Token Listrik Prabayar
Nama Mahasiswa	: Wahdiyah
NIM	: H1051201055
Jurusan/Program Studi	: Rekayasa Sistem Komputer
Tanggal Lulus	: 8 April 2026
SK Pembimbing	: No.3561/UN22.8/TD.06/2024/Tanggal 11 November 2024
SK Penguji	: No.1443/DST/UN22.8/DT.00.09/2026/Tanggal 14 April 2026

Dosen Pembimbing

Pembimbing I	Pembimbing II
Ikhwan Ruslianto, S.Kom., M.Cs.	Kasliono, S.Mat., M.Cs.
NIP. 198607012014041001	NIP. 199306202022031005

Dosen Penguji

Ketua Penguji	Anggota Penguji
Uray Ristian, S.Kom., M.Kom.	Hafiz Muhardi, S.T., M.Kom.
NIP. 199012012019031017	NIP. 199007232023211017

Pimpinan Sidang (merangkap anggota penguji)	Sekretaris Sidang (merangkap anggota sidang)
Ikhwan Ruslianto, S.Kom., M.Cs.	Kasliono, S.Mat., M.Cs.
NIP. 198607012014041001	NIP. 199306202022031005

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	: Wahdiyah
NIM	: H1051201055
Program Studi/ Jurusan	: Rekayasa Sistem Komputer
Fakultas	: Matematika dan Ilmu Pengetahuan

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, 8 April 2026



Wahdiyah

H1051201055

Implementasi Kriptografi *One-Time Pad* untuk Keamanan Pengiriman Data pada Sistem Monitoring Pengisian Token Listrik Prabayar

Abstrak

Perkembangan teknologi yang pesat menjadikan data sebagai aspek penting dalam berbagai sistem modern, termasuk sistem monitoring pengisian token listrik prabayar. Ketergantungan tinggi terhadap data meningkatkan risiko keamanan dan potensi manipulasi yang dapat merusak keaslian informasi. Jika tidak dilindungi dengan baik, data dapat diubah oleh pihak yang tidak berwenang sehingga menimbulkan kesalahan mengambil keputusan. Oleh karena itu, kriptografi diperlukan untuk menjaga keamanan dan integritas data yang dihasilkan. Dalam penelitian ini, algoritma *One-Time Pad* diimplementasikan untuk mengenkripsi data sensor dan kode token yang dihasilkan oleh sistem monitoring token listrik prabayar. Berdasarkan hasil pengujian, rata-rata waktu enkripsi adalah 202,6 µs untuk data sensor dan 81,09 µs untuk data kode token, sedangkan waktu dekripsi rata-rata sebesar 14,50 µs untuk data sensor dan 270 µs untuk data kode token. Pengujian waktu transmisi menunjukkan bahwa rata-rata pengiriman data sensor tanpa enkripsi sebesar 36,98 ms dan meningkat menjadi 68,53 ms setelah enkripsi, sedangkan data kode token meningkat dari 1,70 ms menjadi 2,16 ms. Selain itu, pengujian ketahanan *ciphertext* menggunakan aplikasi *CrypTool* menunjukkan bahwa *ciphertext* dari kedua jenis data tidak dapat dikembalikan ke bentuk *plaintext* asli. Hasil ini membuktikan bahwa algoritma *One-Time Pad* memiliki tingkat keamanan yang sangat tinggi dan efektif dalam mencegah upaya pembacaan maupun manipulasi data oleh pihak yang tidak berwenang.

Kata kunci : *One-Time Pad*, Keamanan Data, Proses Enkripsi, Proses Dekripsi

Implementation of One-Time Pad Cryptography for Data Transmission Security in the Prepaid Electricity Token Replenishment Monitoring System

Abstract

The rapid advancement of technology has made data a crucial aspect of modern systems, including prepaid electricity token monitoring systems. High dependence on data increases security risks and the potential for manipulation that may compromise information authenticity. If data are not properly protected, unauthorized parties may alter them, leading to incorrect decision-making. Therefore, cryptography is required to ensure the security and integrity of the generated data. In this study, the One-Time Pad algorithm is implemented to encrypt sensor data and token codes generated by a prepaid electricity token monitoring system. Based on experimental results, the average encryption time is 202.6 µs for sensor data and 81.09 µs for token code data, while the average decryption time is 14.50 µs for sensor data and 270 µs for token code data. Transmission time testing shows that the average transmission of sensor data without encryption is 36,98 ms and increases to 68.53 ms after encryption, while token code data transmission increases from 1.70 ms to 2.16 ms. Furthermore, ciphertext resistance testing using the CrypTool application demonstrates that the ciphertext of both data types cannot be reverted to their original plaintext form. These results prove that the One-Time Pad algorithm provides a very high level of security and is effective in preventing unauthorized data reading and manipulation.

***Keywords**: One-Time Pad, Data Security, Encryption Process, Decryption Process*

PRAKATA

Alhamdulillah Segala puji dan syukur kepada Allah SWT, atas segala rahmat dan karunia yang melimpah sehingga penulis dapat menyelesaikan tugas akhir yang berjudul "**Implementasi Kriptografi *One-Time Pad* untuk Keamanan Pengiriman Data pada Sistem Monitoring Pengisian Token Listrik Prabayar**". Tujuan dari Penyusunan skripsi ini sebagai salah satu syarat bagi penulis untuk memperoleh gelar Sarjana Komputer pada Jurusan Rekayasa Sistem Komputer Fakultas Matematika dan Pengetahuan Alam Universitas Tanjungpura Pontianak.

Penulis menyadari bahwa dalam penyusunan skripsi ini terdapat banyak bimbingan, petunjuk, saran, maupun dorongan moril dari berbagai pihak. Oleh karena itu, izinkanlah penulis menyampaikan ucapan 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 Suhardi, S.T., M.Eng., selaku dosen Pembimbing Akademik (PA) yang telah dengan sabar memberikan masukan, bimbingan, dan motivasi yang membangun sepanjang masa perkuliahan.
4. Bapak Ikhwan Ruslianto, S.Kom., M.Cs., sebagai dosen Pembimbing Pertama yang telah memberikan masukan, pandangan, serta meluangkan waktu dan pikiran yang ada agar membuat termotivasi dalam bimbingan penulisan skripsi.
5. Bapak Kasliono, S.Mat., M.Cs., sebagai dosen Pembimbing Kedua sekaligus dosen psikolog saya yang telah memberikan masukan, pandangan, serta meluangkan waktu dan pikiran yang ada agar membuat termotivasi dalam bimbingan penulisan skripsi.
6. Bapak Uray Ristian, S.Kom., M.Kom., sebagai dosen Penguji Pertama yang telah memberikan masukan dan pertanyaan yang memberikan peningkatan dalam penulisan skripsi.

7. Bapak Hafiz Muhardi, S.T., M.Kom., sebagai dosen Penguji Kedua yang telah memberikan memberikan masukan dan pertanyaan yang memberikan peningkatan dalam penulisan skripsi.
8. Dosen dan Staf Prodi Rekayasa Sistem Komputer atas pengetahuan dan bantuan yang telah diberikan kepada penulis.
9. Penulis mengucapkan terima kasih yang sebesar-besarnya kepada kedua orang tua dan saudara-saudara tercinta atas doa, dukungan, kasih sayang, serta pengorbanan yang tiada henti dalam setiap langkah penulis menempuh pendidikan hingga penyusunan skripsi ini dapat terselesaikan.
10. Teman-teman Etprofgaktuh yang selalu memberikan semangat dan mendengarkan keluh kesah yaitu Si ana, Linda, dan Dini.
11. Terima kasih untuk GulL Sadoglu, kucing peliharaan yang selalu menemani hari-hari penuh lelah ini, sehat-sehat ya nak.

Pontianak, 8 April 2026



Wahdiyah

DAFTAR ISI

LEMBAR PENGESAHAN ii
PERNYATAAN INTEGRITAS AKADEMIK iii
Abstrak iv
Abstract v
PRAKATA vi
DAFTAR ISI viii
DAFTAR GAMBAR xii
DAFTAR TABEL xiii
DAFTAR KODE PROGRAM xiv
BAB 1 PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Batasan Masalah 4
1.4 Tujuan Penelitian 5
1.5 Manfaat Penelitian 5
1.6 Sistematika Penulisan 6
BAB 2 LANDASAN TEORI 7
2.1 Perbandingan dengan Penelitian terdahulu 7
2.2 Kriptografi 9
2.3 ASCII 9
2.4 One-Time Pad 10
2.5 Selisih 11
2.6 Arduino IDE 12
2.7 Laravel 12
2.8 MySQL 13
2.9 Server 13
2.10 *Bot* Telegram 14
2.11 NodeMCU ESP32 14
2.12 Sensor TCS3200 15

2.13 Servo 15
BAB 3 METODE PENELITIAN 16
3.1 Studi Literatur 16
3.2 Analisis Kebutuhan 17
3.2.1 Kebutuhan Perangkat Keras 17
3.2.2 Kebutuhan Perangkat Lunak 17
3.3 Perancangan Sistem 17
3.4 Implementasi Sistem 18
3.5 Pengujian Sistem 18
3.6 Kesimpulan dan Saran 18
BAB 4 PERANCANGAN 19
4.1 Deskripsi Penelitian 19
4.2 Perancangan Arsitektur Sistem 20
4.3 Perancangan Perangkat Keras 23
4.4 Perancangan Perangkat Lunak 24
4.4.1 Perancangan Proses Enkripsi 24
4.4.2 Perancangan Proses Dekripsi 27
4.5 Perancangan Basis Data 30
4.5.1 Tabel Sensor 30
4.5.2 Tabel Riwayat 31
4.5.3 Tabel Enkripsi Sensor 31
4.5.4 Tabel Enkripsi Token 32
4.6 Perancangan *Bot* Telegram 32
4.7 Perancangan Pengujian 34
4.7.1 Pengujian Waktu Enkripsi pada Data Sensor 34
4.7.2 Pengujian Waktu Dekripsi Pada Data Sensor 34
4.7.3 Pengujian Waktu Enkripsi Pada Kode Token 35
4.7.4 Pengujian Waktu Dekripsi Pada Kode Token 35
4.7.5 Pengujian Pengaruh Algoritma *One-Time Pad* terhadap Waktu Transmisi Data Sensor 35
4.7.6 Pengujian Pengaruh Algoritma *One-Time Pad* terhadap Waktu Transmisi Data Kode Token 36

4.7.7 Pengujian Ketahanan *Ciphertext* Pada Data Sensor dan Kode Token 36
BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN 38
5.1 Implementasi Perangkat Keras 38
5.2 Implementasi Perangkat Lunak 39
5.2.1 Kalibrasi Sensor TCS3200 39
5.2.2 Implementasi Sistem Monitoring pada Keadaan Token 40
5.2.3 Implementasi Algoritma *One-time Pad* Pada Proses Enkripsi Data Sensor 41
5.2.4 Implementasi Algorima *One-time Pad* Pada Proses Dekripsi Data Sensor 43
5.2.5 Implementasi Algoritma *One-time Pad* Pada Proses Enkripsi Kode Token 46
5.2.6 Implementasi Algoritma *One-time Pad* Pada Proses Dekripsi Kode Token 48
5.2.7 Kode Program Perhitungan Waktu Pada Proses Enkripsi Data Sensor TCS3200 50
5.2.8 Kode Program Perhitungan Waktu Pada Proses Dekripsi Data Sensor TCS3200 51
5.2.9 Kode Program Perhitungan Waktu Proses Enkripsi Kode Token .. 51
5.2.10 Kode Program Perhitungan Waktu Pada Proses Dekripsi Data Kode Token 52
5.2.11 Implementasi Bot Telegram 53
5.3 Pengujian Sistem 54
5.3.1 Pengujian Waktu Enkripsi Data Sensor 54
5.3.2 Pengujian Waktu Dekripsi Data Sensor 55
5.3.3 Pengujian Waktu Enkripsi Kode Token 57
5.3.4 Pengujian Waktu Dekripsi Kode Token 59
5.3.5 Pengujian Waktu Transmisi Data Sensor 62
5.3.6 Pengujian Waktu Transmisi Kode Token 64
5.3.7 Uji Ketahanan *Ciphertext* Data Sensor 67
5.3.8 Uji Ketahanan *Ciphertext* Kode Token 69

5.4 Pembahasan 73
BAB 6 PENUTUP 77
6.1 Kesimpulan 77
6.2 Saran 77
DAFTAR PUSTAKA 79
LAMPIRAN 82

DAFTAR GAMBAR

Gambar 2.5 Arduino IDE 12
Gambar 2.2 NodeMCU ESP32 14
Gambar 2.3 Sensor TCS3200 15
Gambar 2. 4 Servo 15
Gambar 3.1 Diagram Alir Penelitian 16
Gambar 4.1 Arsitektur Sistem 20
Gambar 4.2 Diagram Alir Enkripsi, Pengiriman, dan Dekripsi Data Sensor 21
Gambar 4.3 Diagram Alir Enkripsi, Pemgiriman, dan Dekripsi Token 22
Gambar 4.4 Alur Proses Enkripsi 27
Gambar 4.5 Perancangan Proses Dekripsi 28
Gambar 4.6 Alur Proses Dekripsi 30
Gambar 4.7 Pembuatan Bot Telegram 33
Gambar 4.8 Request ID Bot Telegram 34
Gambar 4.9 Pengujian Ketahanan Ciphertext 37
Gambar 4.10 Implementasi Bot Telegram 54
Gambar 5.1 Implementasi Perangkat Keras 38
Gambar 5.2 Implementasi Bot Telegram 53
Gambar 5.3 Grafik Waktu Eksekusi Enkripsi Data Sensor 55
Gambar 5.4 Grafik Waktu Eksekusi Dekripsi Data Sensor 57
Gambar 5.5 Grafik Waktu Eksekusi Enkripsi Kode Token 59
Gambar 5.6 Grafik Waktu Eksekusi Dekripsi Kode Token 61
Gambar 5.7 Grafik Perbandingan Waktu Transmisi Data Sensor 63
Gambar 5.8 Grafik Perbandingan Waktu Transmisi Kode Token 66
Gambar 5.9 CrypTool Ciphertext Data Sensor 67
Gambar 5.10 CrypTool Ciphertext Kode Token 70

DAFTAR TABEL

Tabel 2.1 Perbandingan dengan Penelitian Terdahulu..... 7
Tabel 4.1 Penggunaan Pin di ESP32 24
Tabel 4.2 Perhitungan Proses Enkripsi..... 25
Tabel 4.3 Perhitungan Proses Dekripsi..... 29
Tabel 4.4 Tabel Sensor 30
Tabel 4.5 Tabel Riwayat..... 31
Tabel 4.6 Tabel Enkripsi Sensor..... 31
Tabel 4.7 Tabel Enkripsi Token..... 32
Tabel 5.1 Waktu Enkripsi Data Sensor..... 54
Tabel 5.2 Waktu Dekripsi Data Sensor..... 56
Tabel 5.3 Waktu Enkripsi Kode Token..... 57
Tabel 5.4 Waktu Dekripsi Kode Token..... 60
Tabel 5.5 Waktu Transmisi Data Sensor..... 62
Tabel 5.6 Waktu Transmisi Kode Token..... 65
Tabel 5.7 Uji Ketahanan Ciphertext Data Sensor..... 68
Tabel 5.8 Uji Ketahanan Ciphertext Kode Token 70

DAFTAR KODE PROGRAM

Kode Program 5.1 Kode Program Kalibrasi Sensor TCS3200 39
Kode Program 5.2 Sistem Monitoring pada Keadaan Token..... 41
Kode Program 5.3 Kode Program Proses Enkripsi Data Sensor 42
Kode Program 5.4 Kode Program Proses Dekripsi Data Sensor 44
Kode Program 5.5 Kode Program Proses Enkripsi Kode Token 46
Kode Program 5.6 Kode Program Proses Dekripsi Data Token 48
Kode Program 5.7 Kode Program Waktu Enkripsi Data Sensor 50
Kode Program 5.8 Kode Program Waktu Dekripsi Data Sensor 51
Kode Program 5.9 Kode Program Waktu Enkripsi Kode Token 52
Kode Program 5.10 Kode Program Waktu Dekripsi Kode Token 52

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Listrik merupakan salah satu kebutuhan utama dalam kehidupan sehari-hari yang berperan penting dalam mendukung berbagai aktivitas rumah tangga, industri, maupun perkantoran (Ammarullah, 2024). Penggunaan energi listrik perlu dikelola dan diukur secara akurat agar konsumsi dapat terkontrol dengan baik. Untuk itu, digunakan alat ukur energi listrik yang dikenal sebagai kwh meter. Perkembangan teknologi telah mendorong perubahan dari kwh meter konvensional menjadi kwh meter digital yang lebih modern dan praktis. Kwh meter digital merupakan layanan listrik dari PLN yang menggunakan sistem prabayar, dimana energi listrik dapat digunakan setelah pelanggan melakukan pembelian dan aktivasi token listrik (Darmono & Suharto, 2024). Meskipun sistem ini memberikan kemudahan dalam pengendalian penggunaan listrik, terdapat kendala bagi pelanggan yang sering bepergian yaitu listrik tidak dapat digunakan ketika token telah habis dan informasi sisa token hanya ditampilkan melalui lampu indikator pada meteran. Lampu indikator tersebut akan berubah menjadi merah dan berkedip ketika token hampir habis. Kondisi ini menyebabkan proses pemantauan dan pengisian token tidak dapat dilakukan secara jarak jauh. Kondisi tersebut mendorong perlunya sistem monitoring jarak jauh agar informasi sisa token dapat dipantau secara real-time melalui jaringan komunikasi. Namun, penggunaan jaringan dalam proses pengiriman data menimbulkan permasalahan baru yaitu risiko keamanan data selama transmisi. Salah satu ancaman yang dapat terjadi adalah *sniffing*.

Sniffing merupakan teknik penyadapan jaringan yang dilakukan dengan cara menangkap dan menganalisis paket data yang melintas pada suatu jaringan komunikasi (Ayman & Nurhadiyanto, 2024). Apabila *sniffing* terjadi pada sistem kwh meter berbasis jaringan, maka data penting seperti informasi sisa token maupun kode token berpotensi diketahui atau dimanipulasi oleh pihak yang tidak berwenang. Hal ini dapat menyebabkan penyalahgunaan sistem, kesalahan pembacaan data, hingga gangguan pada proses pengisian token. Oleh karena itu,

diperlukan mekanisme pengamanan untuk melindungi data selama proses transmisi, salah satunya melalui penerapan metode kriptografi.

Kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengubah data asli (*plaintext*) menjadi bentuk tersandi (*ciphertext*) sehingga tidak dapat dipahami oleh pihak yang tidak memiliki kunci (Harahap & Khairina, 2018). Dalam sistem monitoring kwh meter digital, kriptografi berperan untuk menjaga kerahasiaan dan integritas data yang dikirimkan dari perangkat ke *server* agar tetap aman meskipun data tersebut berhasil ditangkap melalui proses *sniffing*. Penerapan kriptografi diperlukan untuk mencegah penyadapan dan manipulasi data selama proses komunikasi jaringan. Pada penelitian ini, metode kriptografi yang digunakan adalah algoritma *One-Time Pad*. Algoritma *One-Time Pad* adalah algoritma kunci simetris yang menggunakan kunci acak dan hanya digunakan satu kali untuk setiap proses enkripsi (Manalu, 2022). Algoritma ini dipilih karena memiliki tingkat keamanan yang sangat tinggi dan secara teoritis tidak dapat dipecahkan tanpa mengetahui kunci yang digunakan.

Penelitian mengenai metode *One-Time Pad* sebelumnya pernah dilakukan dengan judul "Implementasi Kriptografi pada Aplikasi Diary Berbasis Android menggunakan Algoritma *One-Time Pad*". Penelitian ini merancang dan membangun aplikasi diary berbasis Android yang menerapkan algoritma *One-Time Pad* sebagai metode pengamanan data. Pada penelitian tersebut, setiap catatan yang ditulis pengguna dienkripsi terlebih dahulu sebelum disimpan ke dalam basis data, kemudian dapat didekripsi kembali menggunakan kunci yang sama saat ingin dibaca. Hasil penelitian menunjukkan bahwa algoritma *One-Time Pad* berhasil diimplementasikan dengan baik, di mana proses enkripsi dan dekripsi berjalan sesuai prosedur serta mampu menjaga kerahasiaan data *diary* dari akses yang tidak sah (Saragih & Harahap, 2020).

Penelitian selanjutnya yang berjudul "Implementasi Algoritma One-Time Pad untuk Enkripsi dan Dekripsi pada Peresepan Data Obat di Puskesmas Purwodiningratan Surakarta". Penelitian membuat aplikasi peresepan yang aman dengan menerapkan algoritma *One-Time Pad* sebagai metode kriptografi untuk melakukan proses enkripsi dan dekripsi data resep obat di Puskesmas Purwodiningratan Surakarta. Resep obat merupakan informasi sensitif yang harus

dirahasiakan karena berisi takaran dosis dan jenis obat, sehingga berpotensi disalahgunakan apabila tidak dilindungi. Untuk itu, algoritma *One-Time Pad* digunakan untuk menyandikan data resep menjadi bentuk *ciphertext* guna menjaga kerahasiaan informasi sebelum disimpan atau dikirimkan (Fitriyadi & Ahwan, 2023).

Penelitian selanjutnya yang berjudul "Perancangan Sistem Pengisi Token Listrik Berumpan Balik pada Kwh Meter Prabayar Berbasis Arduino". Pada penelitian ini menghasilkan sebuah sistem yang dapat mengisi token listrik menggunakan perangkat android dengan menerapkan sistem umpan balik pada implementasinya. Penelitian ini mennggunakan arduino sebagai mikroprosesor serta servo yang digunakan sebagai akuator penekan tombol, sistem yang dibangun dapat mengatasi masalah sulitnya pengisian token akibat posisi kwh meter yang tinggi dengan kontrol perangkat android dengan jarak 9-10 meter. Serta memberikan umpan balik ketika terjadi kesalahan. Pada penelitian ini belum ada membahas keamanan sistemnya (Nursalim et al., 2023).

Berdasarkan penelitian yang telah dilakukan, maka diangkatlah penelitian yang berjudul **"Implementasi Kriptografi *One-Time Pad* untuk Keamanan Pengiriman Data pada Sistem Monitoring Pengisian Token Listrik Prabayar"**. Pada penelitian ini dikembangkan sebuah sistem pengamanan dengan mengimplementasikan algoritma kriptografi *One-Time Pad* pada sistem monitoring token listrik guna mencegah serangan *active sniffing* yang berpotensi mengubah data sensor warna TCS3200 maupun kode token yang dikirimkan melalui jaringan. Data sensor berupa nilai RGB dari cahaya lampu indikator kWh meter, di mana indikator berwarna hijau menunjukkan token masih tersedia dalam jumlah cukup, sedangkan indikator berwarna merah menunjukkan sisa token hampir habis. Data sensor tersebut perlu diamankan karena apabila tidak dilindungi, pihak yang tidak bertanggung jawab dapat memanipulasi nilai sensor sehingga sistem menampilkan kondisi token yang tidak sesuai dengan keadaan sebenarnya. Hal ini dapat menyebabkan kesalahan pengambilan keputusan oleh pengguna, khususnya dalam menentukan waktu pengisian ulang token listrik. Kesalahan tersebut berpotensi menimbulkan kerugian, terutama pada lokasi yang membutuhkan suplai listrik

secara terus-menerus. Selain itu, pengiriman kode token juga harus diamankan agar tidak dapat disadap maupun dimodifikasi selama proses transmisi.

Penelitian ini tidak hanya berfokus pada implementasi algoritma, tetapi juga menganalisis waktu yang dibutuhkan dalam proses enkripsi dan dekripsi, membandingkan waktu transmisi data sebelum dan sesudah penerapan kriptografi, serta menguji ketahanan *ciphertext* dalam menjaga kerahasiaan dan keaslian data. Hasil penelitian menunjukkan bahwa waktu eksekusi enkripsi dan dekripsi yang dilakukan di *server* lebih cepat dibandingkan pada ESP32, waktu transmisi data mengalami peningkatan setelah diterapkan enkripsi dibandingkan pengiriman tanpa enkripsi, serta *ciphertext* yang dihasilkan algoritma *One-Time Pad* tidak dapat didekripsi baik pada data sensor maupun kode token, sehingga mampu menjaga kerahasiaan informasi yang dikirimkan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka permasalahan yang didapat pada penelitian ini adalah

1. Bagaimana waktu yang dibutuhkan dalam proses enkripsi dan dekripsi menggunakan algoritma *One-Time Pad* pada sistem monitoring pengisian token listrik prabayar ?
2. Bagaimana perbandingan waktu transmisi data pada sistem monitoring pengisian token listrik sebelum dan sesudah penerapan algoritma *One-Time Pad* ?
3. Bagaimana ketahanan *ciphertext* yang dihasilkan oleh algoritma *One-Time Pad* dalam menjaga kerahasiaan dan keaslian data pada sistem monitoring pengisian token listrik prabayar ?

1.3 Batasan Masalah

Batasan masalah dibuat agar maksud dan tujuan dari penelitian dapat terfokus sesuai dengan tujuan. Adapun batasan masalah dalam penelitian ini antara lain sebagai berikut.

1. Penelitian ini berfokus pada penggunaan algoritma dalam mengamankan data sensor dan kode token pada sistem monitoring pengisian token listrik prabayar.
2. Penelitian ini berfokus mengamankan data sensor warna TCS3200 yang digunakan untuk mendeteksi kondisi token listrik.
3. Penelitian ini hanya menggunakan nilai warna merah dan hijau dari sensor TCS3200, sedangkan nilai warna lainnya tidak digunakan.
4. Penelitian ini berfokus mengamankan data kode token yang akan dikirim dari *server* ke ESP32.
5. Penelitian tidak akan membahas aspek implementasi fisik dari sistem monitoring token listrik prabayar, fokusnya hanya pada penggunaan algoritma *One-Time Pad* dalam mengamankan data sensor dan kode token.
6. Sistem notifikasinya menggunakan *bot* telegram.

1.4 Tujuan Penelitian

Berdasarkan permasalahan yang didapat, tujuan dari penelitian ini adalah

1. Dapat mengetahui waktu yang diperlukan pada proses enkripsi dan dekripsi algoritma *One-Time Pad* pada sistem monitoring pengisian token listrik prabayar.
2. Dapat mengetahui pengaruh algoritma *One-Time Pad* terhadap waktu transmisi data pada sistem monitoring pengisian token listrik prabayar.
3. Dapat mengetahui ketahanan algoritma *One-Time Pad* dalam menjaga kerahasiaan dan keaslian data pada sistem monitoring pengisian token listrik prabayar.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat meningkatkan keamanan data sensor pada sistem monitoring token listrik prabayar dengan mengimplementasikan algoritma *One-Time Pad* sehingga dapat mencegah serangan yang dapat mengubah data. Hasil dari penelitian ini dapat menjadi panduan bagi pengembang dalam menyeimbangkan keamanan dan kinerja sistem monitoring berbasis IoT, serta menambah wawasan ilmiah di bidang keamanan data IoT. Secara keseluruhan,

penelitian ini diharapkan dapat meningkatkan kepercayaan pengguna terhadap sistem monitoring token listrik dan mendorong adopsi teknologi yang lebih luas dan aman.

1.6 Sistematika Penulisan

Sistematika penulisan pada penelitian ini terdiri dari beberapa bagian yang meliputi :

BAB 1 PENDAHULUAN

Bab pendahuluan berisi tentang latar belakang yang menjadi dasar penelitian, perumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, dan sistematika penulisan sehingga mendapat gambaran umum pada setiap bab.

BAB 2 LANDASAN TEORI

Bab landasan teori berisi bahasan mengenai dasar teori pendukung yang digunakan dalam tugas akhir. Adapun landasan teori pada bab ini berupa dasar teori Kriptografi, ASCII (*American Standard Code for International Interchange*, *One-Time Pad*, NodeMCU ESP32, Sensor TCS3200, Servo, Arduino IDE, Laravel, MySQL, Server, Bot Telegram.

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, pengumpulan data, analisis kebutuhan, perancangan sistem, implementasi, pengujian sistem, analisis, kesimpulan dan saran.

BAB 4 PERANCANGAN

Bab perancangan merupakan bagian dari penelitian yang menjelaskan tentang rancangan sistem yang dibangun meliputi perancangan pada perangkat keras dan perangkat lunak. Perancangan sistem meliputi penjelasan tentang deskripsi sistem, perancangan arsitektur sistem, perancangan perangkat keras, perancangan perangkat lunak yang terdiri dari perancangan proses enkripsi dan perancangan proses dekripsi, perancangan basis data, perancangan antar muka serta perancangan pengujian.

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Bab implementasi, pengujian, dan pembahasan berisi tahapan-tahapan yang dilakukan untuk mengimplementasikan, menguji dan membahas sistem. Tahapan implementasi, pengujian dan pembahasan terdiri dari implementasi sistem, kode program, pengujian sistem dan hasil sistem. Setelah dilakukan pengujian maka dilakukan pembahasan dari hasil pengujian keseluruhan sistem.

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.