IMPLEMENTASI KRIPTOGRAFI *ONE-TIME PAD* (*XOR*) UNTUK PENGIRIMAN DATA PADA SISTEM *SMART DOOR* BERBASIS *IOT* DENGAN *QR CODE*

MUHAMMAD DITO ASROFA
H1051211005

SKRIPSI

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2025

IMPLEMENTASI KRIPTOGRAFI *ONE-TIME PAD* (*XOR*) UNTUK PENGIRIMAN DATA PADA SISTEM *SMART DOOR* BERBASIS *IOT* DENGAN *QR CODE*

Muhammad Dito Asrofa
H1051211005

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
2025

LEMBAR PENGESAHAN

Judul Tugas Akhir	: Implementasi Kriptografi One-Time Pad (Xor) untuk Pengiriman Data pada Sistem *Smart Door* Berbasis IoT dengan *QR Code*
Nama Mahasiswa	: Muhammad Dito Asrofa
NIM	: H105121105
Jurusan/Program Studi	: Rekayasa Sistem Komputer
Tanggal Lulus	: 25 Juli 2025
SK Pembimbing	: No.262/UN22.8/TD.06/2025 /Tanggal 3 Februari 2025
SK Penguji	: No.2260/UN22.8/TD.06/2025 /Tanggal 17 Juli 2025

Dosen Pembimbing

Pembimbing I	Pembimbing II
Syamsul Bahri, S.Kom., M.Cs.	Kasliono, S.Mat., M.Cs.
NIP. 198802272015041001	NIP. 199306202022031005

Dosen Penguji

Ketua Penguji	Anggota Penguji
Ikhwan Ruslianto, S.Kom., M.Cs.	Hirzen Hasfani, S.Kom., M.Cs.
NIP. 198607012014041001	NIP. 199305032022031003

Pimpinan Sidang (merangkap anggota penguji)	Sekretaris Sidang (merangkap anggota penguji)
Syamsul Bahri, S.Kom., M.Cs.	Kasliono, S.Mat., M.Cs.
NIP. 198802272015041001	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	: Muhammad Dito Asrofa
NIM	: H1051211005
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, 25 Juli 2025

Meterai

Muhammad Dito Asrofa
NIM. H105121005

Implementasi Kriptografi One-Time Pad (XOR) untuk Pengiriman Data pada Sistem Smart Door Berbasis IoT dengan QR Code

Abstrak

Meningkatnya penggunaan Internet of Things (IoT) pada sistem Smart Door mendorong kebutuhan akan pengamanan data autentikasi, khususnya terhadap serangan sniffing. Namun, sebagian besar komunikasi data dalam sistem IoT masih belum dilengkapi dengan enkripsi yang kuat. Penelitian ini bertujuan untuk mengamankan sistem Smart Door berbasis QR Code dengan menerapkan algoritma One-Time Pad (OTP) XOR pada tiga jalur komunikasi utama: server ke website pengguna, ESP32-CAM ke server, dan server ke NodeMCU ESP32. Algoritma OTP XOR menghasilkan ciphertext yang berbeda untuk setiap pengiriman meskipun plaintext-nya sama, berkat penggunaan kunci acak satu kali pakai. Hasil pengujian menunjukkan bahwa data terenkripsi tidak dapat diungkap melalui sniffing ataupun kriptanalisis menggunakan tools seperti Wireshark dan dCode.fr. Selain itu, waktu proses enkripsi dan dekripsi tergolong cukup cepat, dengan rata-rata 0.011 ms di server, 0.010 ms di website pengguna, 0.345 ms di ESP32-CAM, dan 0.166 ms di ESP32. Hasil ini menunjukkan bahwa algoritma OTP XOR dapat diimplementasikan secara baik pada perangkat IoT yang memiliki keterbatasan sumber daya, untuk menghadirkan sistem Smart Door yang cepat dan aman.

Kata kunci: Pintu Pintar, IoT, *QR Code*, Kriptografi, One-Time Pad, XOR, Keamanan Data.

Implementation of One-Time Pad (XOR) Cryptography for Data Transmission in IoT-Based Smart Door Systems with QR Code

Abstract

The increasing use of the Internet of Things (IoT) in Smart Door systems drives the need for authentication data security, especially against sniffing attacks. However, most data communications in IoT systems are still not equipped with strong encryption. This study aims to secure a QR Code-based Smart Door system by implementing the One-Time Pad (OTP) XOR algorithm on three main communication paths: server to user website, ESP32-CAM to server, and server to NodeMCU ESP32. The OTP XOR algorithm produces different ciphertexts for each transmission even though the plaintext is the same, thanks to the use of a one-time random key. Test results show that encrypted data cannot be revealed through sniffing or cryptanalysis using tools such as Wireshark and dCode.fr. In addition, the encryption and decryption process times are quite fast, with an average of 0.011 ms on the server, 0.010 ms on the user website, 0.345 ms on the ESP32-CAM, and 0.166 ms on the ESP32. These results show that the OTP XOR algorithm can be implemented well on IoT devices that have limited resources, to provide a fast and secure Smart Door system.

Keywords: *Smart Door, IoT, QR Code, Cryptography, One-Time Pad, XOR, Data Security*

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 Kriptografi One-Time Pad (Xor) untuk Pengiriman Data pada Sistem *Smart Door* Berbasis IoT dengan *QR Code*"** 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. Bapak Tedy Rismawan, S.Kom., M.Cs., selaku Ketua Jurusan Rekayasa Sistem Komputer FMIPA Universitas Tanjungpura Pontianak.
3. Bapak Syamsul Bahri, S.Kom., M.Cs., sebagai dosen Pembimbing Pertama yang telah memberikan masukan serta meluangkan waktu dan pikiran yang memberikan dorongan dalam bimbingan penulisan skripsi.
4. Bapak Kasliono, S.Mat.,M.Cs., sebagai dosen Pembimbing Kedua yang telah memberikan masukan serta meluangkan waktu dan pikiran yang memberikan dorongan dalam bimbingan penulisan skripsi.
5. Bapak Ikhwan Ruslianto, S.Kom., M.Cs., selaku dosen Penguji Pertama, yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini
6. Bapak Hirzen Hasfani, S.Kom., M.Cs., selaku dosen Penguji Kedua, yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.
7. Ibu Rahmi Hidayati, S.Kom., M.Cs., sebagai dosen Pembimbing Akademik (PA) yang telah memberi masukan dan motivasi yang membangun selama masa perkuliahan.

8. Kepada orang tua dan keluarga yang selalu memberikan dukungan, doa, motivasi, dan kasih sayang tanpa henti sepanjang perjalanan penulisan tugas akhir ini.
9. 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.
10. Teman-teman dekat yang memberi semangat dan saran dalam tugas akhir ini sehingga dapat terselesaikan.
11. Semua pihak yang terlibat langsung maupun yang tidak langsung dalam penulisan tugas akhir ini.

Pontianak,

Muhammad Dito Asrofa

DAFTAR ISI

LEMBAR PENGESAHAN iii
PERNYATAAN INTEGRITAS AKADEMIK ii
Abstrak iv
Abstract v
PRAKATA vi
DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xii
DAFTAR KODE PROGRAM xiii
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 5
BAB 2 LANDASAN TEORI 7
2.1 Perbandingan dengan penelitian terdahulu 7
2.2 Internet Of Things (IoT) 8
2.3 Kriptografi 8
2.4 One-Time pad 9
2.5 Sniffing 10
2.6 NodeMCU ESP32 11
2.7 ESP32-CAM 12
2.8 *Solenoid Door Lock* 12
2.9 *Universally Unique Identifier (UUID)* 13
2.10 *Cloud Server* 13
2.11 Arduino IDE 14
2.12 Laravel 15
2.13 Ettercap 15

2.14 Wireshark 16
2.15 dCode.fr 17
2.16 Balsamiq Mockup 17
2.17 Diagram Alir (*Flowchart)* 18
BAB 3 METODE PENELITIAN 19
3.1 Studi Literatur 19
3.2 Analisis Kebutuhan 20
3.2.1 Kebutuhan Perangkat Keras 20
3.2.2 Kebutuhan Perangkat Lunak 20
3.3 Perancangan Sistem 21
3.3.1 Perancangan Perangkat Keras 21
3.3.2 Perancangan Perangkat Lunak 21
3.4 Implementasi 21
3.5 Pengujian 21
3.6 Data Hasil Pengujian 22
3.7 Kesimpulan dan Saran 22
BAB 4 PERANCANGAN 23
4.1 Deskripsi Sistem 23
4.2 Perancangan Arsitektur Sistem 24
4.3 Perancangan Perangkat Keras 25
4.4 Perancangan Perangkat Lunak 28
4.5 Perancangan Algoritma OTP XOR 29
4.6 Perancangan Basis Data 33
4.6.1 Tabel Users 33
4.6.2 Tabel Pengguna 33
4.6.3 Tabel Qrcode_result 34
4.6.4 Tabel Command_queues 34
4.6.5 Tabel Encryption_timings 35
4.7 Perancangan Antar Muka 35
4.7.1 Perancangan Antarmuka *Website Admin* 35
4.7.2 Perancangan Antarmuka Website User 37
4.8 Perancangan Pengujian Algoritma OTP XOR 38

4.9 Perancangan Pengujian Waktu Proses Enkripsi dan Dekripsi 40
BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN..... 41
5.1 Implementasi Perangkat Keras 41
5.2 Implementasi Perangkat Lunak 42
5.2.1 Tampilan Halaman Hasil Pembacaan *QR Code*..... 45
5.2.2 Tampilan Halaman Log History..... 45
5.2.3 Tampilan Halaman Waktu Proses..... 46
5.2.4 Tampilan Halaman Dashboard Pengguna..... 46
5.3 Implementasi Algoritma OTP XOR 47
5.4 Pengujian Sistem 57
5.4.1 Pengujian Algoritma OTP XOR 57
5.4.2 Pengujian Waktu Proses Enkripsi dan Dekripsi..... 69
5.5 Pembahasan 74
BAB 6 PENUTUP..... 77
6.1 Kesimpulan.....77
6.2 Saran 77
DAFTAR PUSTAKA 79
LAMPIRAN..... 83

DAFTAR GAMBAR

Gambar 2.1 Algoritma OTP secara umum 10
Gambar 2.2 NodeMCU ESP32 12
Gambar 2.3 ESP32-CAM 12
Gambar 2.4 *Solenoid Door Lock* 13
Gambar 2.5 Cara Kerja *Cloud Server* 14
Gambar 2.6 Arduino IDE 15
Gambar 3. 1 Diagram Alir Penelitian 19
Gambar 4.1 Arsitektur Sistem Smart Door 24
Gambar 4.2 Rancangan Skema Perangkat keras 27
Gambar 4.3 Diagram Alir Sistem Smart Door 29
Gambar 4.4 Diagram Alir Proses Enkripsi 30
Gambar 4.5 Diagram Alir Proses Dekripsi 31
Gambar 4.6 Diagram Alir Proses Keseluruhan Algoritma OTP 32
Gambar 4.7 Rancangan Tampilan Halaman Hasil Pembacaan *QR Code* 36
Gambar 4.8 Rancangan Tampilan Halaman Log History 37
Gambar 4.9 Rancangan Tampilan Halaman Waktu Proses 37
Gambar 4.10 Rancangan Tampilan Halaman *Dashboard* Web User 38
Gambar 5.1 Impelementasi Perangkat Keras 41
Gambar 5.2 Tampilan Halaman Pembacaan *QR Code* 45
Gambar 5.3 Tampilan Halaman Log History 46
Gambar 5.4 Tampilan Halaman Waktu Proses 46
Gambar 5.5 Tampilan Halaman Dashboard Pengguna 47
Gambar 5.6 Pengujian Chiper Identifier 63
Gambar 5.7 Pengujian XOR Cipher 67
Gambar 5.8 Tampilan Data Pengujian Waktu Proses 69
Gambar 5.9 Speedtest Jaringan 69
Gambar 5.10 Grafik Waktu Proses Enkripsi Pada ESP32-CAM 72
Gambar 5.11 Grafik Waktu Proses Dekripsi pada Server Jalur 2 72
Gambar 5.12 Grafik Waktu Proses Enkripsi Pada Server Jalur 3 74
Gambar 5.13 Grafik Waktu Proses Dekripsi pada ESP32 74

DAFTAR TABEL

Tabel 4.1 Penggunaan Pin ESP32 dengan relay dan buzzer 27
Tabel 4.2 Penggunaan Pin Relay dengan *Solenoid Door Lock* dan Jack Female . 27
Tabel 4.3 Penggunaan Pin *Solenoid Door Lock* dengan Jack Female 28
Tabel 4.4 Rancangan Tabel Users 33
Tabel 4.5 Rancangan Tabel Pengguna 34
Tabel 4.6 Rancangan Tabel Qrcode_result 34
Tabel 4.7 Rancangan Tabel command_queues 35
Tabel 4.8 Rancangan Tabel encryption_timings 35
Tabel 5.1 Konversi Hex ke Biner 48
Tabel 5.2 Perhitungan Pada Byte 0 49
Tabel 5.3 Perhitungan XOR Pada Byte 1 49
Tabel 5.4 Hasil XOR Lengkap 50
Tabel 5.5 Proses Dekripsi 51
Tabel 5.6 Pengujian Algoritma OTP XOR untuk Pengiriman Data Autentikasi .. 58
Tabel 5.7 Pengujian Algoritma OTP XOR untuk Pengiriman data QR Code 60
Tabel 5.8 Pengujian Algoritma OTP XOR untuk Pengiriman Intruksi ESP32 62
Tabel 5.9 Pengujian Waktu Enkripsi dan Dekripsi Data Autentikasi 70
Tabel 5.10 Pengujian Waktu Enkripsi dan Dekripsi Data Pembacaan QR Code . 71
Tabel 5.11 Pengujian Waktu Enkripsi dan Dekripsi Data Instruksi 73

DAFTAR KODE PROGRAM

Kode Program 5.1 Kode Program Pembacaan *QR Code* pada ESP32-CAM 42
Kode Program 5.2 Kode Program Verifikasi UUID di Server 43
Kode Program 5.3 Kode Program Menerima Perintah dari Server pada ESP32 .. 44
Kode Program 5.4 Mengaktifkan Solenoid Door Lock 44
Kode Program 5.5 Mengaktifkan Buzzer..... 44
Kode Program 5.6 Enkripsi UUID di Server 52
Kode Program 5.7 Dekripsi UUID di Website Pengguna..... 52
Kode Program 5.8 Enkripsi Hasil Pembacaan QR Code 53
Kode Program 5.9 Dekripsi Hasil Pembacaan QR Code..... 54
Kode Program 5.10 Enkripsi Perintah Instruksi 55
Kode Program 5.11 Dekripsi Instruksi pada ESP32 56

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) merupakan konsep yang memungkinkan benda fisik terhubung ke internet untuk saling berkomunikasi dan bertukar data. Teknologi ini tidak hanya memungkinkan pengumpulan data, tetapi juga penggunaannya untuk meningkatkan dan kenyamanan dalam berbagai aspek kehidupan manusia. Salah satu penerapannya dapat ditemukan pada sistem *Smart Lock Door*, di mana teknologi IoT digunakan untuk meningkatkan keamanan dan kenyamanan melalui pengelolaan akses pintu secara cerdas (Juniawan & Rismayana, 2024). Dengan teknologi ini, pengguna dapat mengelola akses pintu dengan lebih aman dan efisien, memungkinkan pemilik rumah atau pengelola gedung untuk memberikan hak akses yang sesuai kepada setiap individu.

Dalam sistem *Smart Door*, *QR code* telah digunakan sebagai media autentikasi yang memungkinkan proses verifikasi akses berjalan lebih cepat dan efisien. Kode unik yang berisi kredensial pengguna dipindai oleh perangkat khusus, diverifikasi melalui server pusat, dan memastikan akses hanya diberikan kepada individu yang memiliki otorisasi, sehingga meningkatkan keamanan dan kenyamanan pengguna (Adedoyin & Olukoya, 2024).

Namun, meskipun menawarkan efisiensi, sistem ini tidak terlepas dari tantangan keamanan. Sebanyak 98% lalu lintas antar perangkat IoT dilaporkan tidak terenkripsi, sehingga rentan terhadap ancaman seperti *Man-in-the-Middle* (MitM) dan kebocoran data yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab (Fereidouni et al., 2023). Hal ini memungkinkan penyadapan dan modifikasi data yang dikirim antara perangkat dan server. Selain itu, komunikasi perangkat-server sering kali rentan terhadap serangan *sniffing* paket data, sehingga informasi sensitif seperti kata sandi dan PIN dapat terekspos jika tidak dienkripsi dengan baik (Lantz & Pierrou, 2022). Untuk mengatasi tantangan ini, algoritma One-Time Pad (OTP) XOR dapat diterapkan. Dengan kunci enkripsi yang unik dan hanya digunakan satu kali di setiap sesi komunikasi.

Peningkatan keamanan pada sistem *Smart Door* melalui penerapan algoritma kriptografi dapat memunculkan tantangan pada kebutuhan sumber daya perangkat. Tercatat kenaikan waktu proses sebesar 0,81%, penggunaan CPU 18%, penggunaan data 5,3%, dan penggunaan memori keseluruhan proses 5,04% akibat implementasi keamanan dapat terjadi (Adhiwibowo et al., 2022). Dalam sistem *Smart Door* waktu yang muncul dari pemrosesan data terenkripsi ini perlu menjadi perhatian. Mengingat kapabilitas komputasi perangkat IoT yang terbatas, efisiensi waktu proses enkripsi dan dekripsi menjadi krusial agar sistem *Smart Door* dapat beroperasi secara cepat dan responsif, tanpa menimbulkan penundaan signifikan bagi pengguna. Oleh karena itu, waktu proses enkripsi dan dekripsi OTP XOR pada perangkat ESP32 dalam sistem *Smart Door* berbasis IoT perlu diukur untuk memastikan bahwa proses algoritma kriptografi tidak menimbulkan waktu yang lama.

Untuk mengatasi masalah ini, diterapkan algoritma One-Time Pad (OTP) dalam sistem *Smart Door* berbasis IoT. Algoritma One-Time Pad (OTP) digunakan untuk mengamankan pengiriman data antara website pengguna, perangkat ESP32-CAM dan server. Dengan penerapan OTP, data autentikasi dan perintah sistem dienkripsi menggunakan kunci unik yang hanya berlaku untuk satu sesi komunikasi. Penerapan OTP ini diharapkan tidak akan memakan waktu proses enkripsi dan dekripsi yang lama. Hal ini karena algoritma OTP hanya menggunakan operasi XOR bitwise yang sederhana. Operasi logika XOR yang sederhana memungkinkan implementasi pada perangkat mikrokontroler dengan sumber daya terbatas seperti ESP32-CAM dan NodeMCU ESP32 tanpa menimbulkan penundaan signifikan dalam sistem *Smart Door*.

Penelitian sebelumnya yang berjudul "Sistem Pintu Cerdas dengan QR Code berbasis Internet of Things sebagai Penerapan Edge Computing" (Hakim & Ristian, 2023). Penelitian ini merancang sistem pintu cerdas yang menggunakan teknologi QR Code sebagai metode autentikasi dan menerapkan Edge Computing untuk mengurangi ketergantungan terhadap koneksi internet. Sistem ini menggunakan ESP32-CAM untuk pemindaian QR Code dan mengandalkan komunikasi lokal melalui Edge Server. Fitur penjadwalan akses juga ditambahkan untuk meningkatkan fleksibilitas kontrol. Hasil pengujian menunjukkan bahwa sistem

mampu beroperasi dengan baik dalam kondisi normal maupun offline, dengan rata-rata delay sekitar 3,35 detik pada mode normal dan 3,01 detik pada mode offline, menunjukkan bahwa pendekatan ini dapat meningkatkan efisiensi dan responsivitas sistem pintu cerdas berbasis IoT.

Penelitian selanjutnya yang berjudul "Cryptography With One-Time Pad (OTP) Algorithm XOR Based" (Manullang et al., 2024). Penelitian ini membahas konsep dasar algoritma OTP yang menggunakan kunci acak dengan panjang yang sama seperti pesan asli (plaintext), dan proses enkripsi serta dekripsi dilakukan melalui operasi XOR. Studi ini juga memaparkan bagaimana OTP mampu menghasilkan ciphertext yang tidak dapat dipecahkan tanpa mengetahui kunci yang digunakan, serta mendemonstrasikan penerapannya secara manual dan menggunakan Python. Meskipun OTP terbukti sangat aman secara teori karena sifat kunci yang acak dan hanya digunakan satu kali, studi ini juga menyoroti tantangan utama pada manajemen dan distribusi kunci dalam implementasi nyata. Dengan demikian, penelitian ini memperkuat pentingnya algoritma OTP dalam menjaga kerahasiaan dan integritas data, khususnya dalam komunikasi pada sistem yang memerlukan tingkat keamanan tinggi seperti IoT.

Penelitian selanjutnya yang berjudul "Pengamanan Kunci Pintu Brankas Menggunakan Kriptografi One Time Pad (OTP) Berbasis Android" (Asih & Hasibuan, 2023) berfokus pada penerapan algoritma OTP untuk meningkatkan keamanan data autentikasi pada sistem penguncian brankas. OTP digunakan untuk mengenkripsi password sebelum disimpan, sehingga data tetap aman meskipun perangkat fisik dibobol. Algoritma ini memastikan bahwa setiap kunci hanya dapat digunakan satu kali, sehingga data yang dienkripsi tidak dapat diakses tanpa kunci yang sesuai. Hasil penelitian menunjukkan bahwa penerapan OTP efektif dalam menjaga kerahasiaan data dan melindungi sistem dari potensi manipulasi atau penyadapan.

Berdasarkan penelitian sebelumnya, maka diangkat sebuah penelitian yang berjudul "Implementasi Kriptografi One-Time Pad XOR untuk Pengiriman Data pada Sistem Smart Door Berbasis IoT dengan QR Code". Penelitian ini bertujuan untuk mengamankan jalur pengiriman data antara aplikasi, server, ESP32-CAM, dan NodeMCU ESP32 pada sistem *Smart Door* berbasis IoT. Data yang dikirim

akan dienkripsi menggunakan algoritma One-Time Pad XOR, sehingga hanya pihak yang berwenang yang dapat mendekripsi dan mengakses informasi tersebut. Dengan penerapan algoritma ini, diharapkan dapat mengurangi risiko penyalahgunaan data akibat penyadapan serta meningkatkan kerahasiaan dan keandalan transmisi informasi dalam sistem IoT yang digunakan untuk pengelolaan akses pintu secara cerdas.

1.2 Rumusan Masalah

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

1. Bagaimana ketahanan algoritma One-Time Pad (OTP) terhadap dampak serangan sniffing dan upaya kriptanalisis dalam sistem Smart Door berbasis IoT?
2. Bagaimana waktu proses enkripsi dan dekripsi OTP XOR pada perangkat ESP32 dalam sistem *Smart Door* berbasis IoT dengan *QR Code*?

1.3 Batasan Masalah

Batasan masalah penelitian ini adalah sebagai berikut:

1. Penelitian ini hanya akan mengembangkan sistem *Smart Door* berbasis IoT yang menggunakan NodeMCU ESP32 sebagai perangkat pengendali dan ESP32 CAM untuk proses pembacaan *QR code*.
2. Performa sistem dilakukan dengan mengukur waktu proses enkripsi dan dekripsi pada perangkat ESP32-CAM dan NodeMcu ESP32 pada saat mengirim data.
3. Penelitian ini tidak akan membahas keamanan pada infrastruktur server, tetapi hanya fokus pada keamanan di perangkat IoT *Smart Door*.
4. Penelitian ini hanya akan mengamankan jalur pengiriman data pada sistem *Smart door*.
5. Data yang diamankan ada pada 3 jalur yaitu dari server ke aplikasi, ESP32-CAM ke server dan dari server ke NodeMcu ESP32.
6. Penelitian ini dibatasi pada pengamanan data komunikasi terhadap dampak serangan *sniffing* melalui penerapan algoritma OTP XOR.

7. Menggunakan Arduino IDE untuk pemrograman pada perangkat keras.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menerapkan algoritma One-Time Pad (OTP) XOR untuk menjaga kerahasiaan data komunikasi pada sistem *Smart Door* berbasis IoT.
2. Mengukur waktu proses enkripsi dan dekripsi OTP (XOR) pada ESP32 untuk mengetahui kebutuhan waktu pemrosesan pada sistem *Smart Door*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah memberikan kontribusi dalam meningkatkan keamanan komunikasi data pada sistem *Smart Door* berbasis Internet of Things (IoT). Dengan menerapkan algoritma kriptografi One-Time Pad (OTP) XOR, data yang ditransmisikan dalam sistem dapat dienkripsi dengan kunci acak yang unik pada setiap sesi. Hal ini memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang, serta mendukung terciptanya sistem yang lebih aman, handal, dan terlindungi dari potensi ancaman selama proses transmisi data berlangsung.

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 ini berisi latar belakang yang menjelaskan tentang permasalahan keamanan pengiriman data pada sistem *Smart Door* berbasis IoT, serta alasan pentingnya penerapan algoritma kriptografi One-Time Pad (OTP) XOR. Selain itu, bab ini juga memuat rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

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 Internet of Things (IoT), Kriptografi, One-Time pad, NodeMCU ESP32, ES32-CAM,

Solenoid Door Lock, Universally Unique Identifier (UUID), *Cloud Server*, Laravel, Balsamiq Mockup, Diagram Alir.

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

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.