IMPELEMENTASI KRIPTOGRAFI VIGENERE CIPHER UNTUK KEAMANAN PENGIRIMAN DATA PADA SISTEM *SMART DOOR* BERBASIS IOT DENGAN *QR CODE*

RISKI ARASYID
H1051211025

SKRIPSI

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

IMPELEMENTASI KRIPTOGRAFI VIGENERE CIPHER UNTUK KEAMANAN PENGIRIMAN DATA PADA SISTEM *SMART DOOR* BERBASIS IOT DENGAN *QR CODE*

RISKI ARASYID
H1051211025

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 Vigenere Cipher untuk Keamanan Pengiriman Data pada Sistem *Smart Door* Berbasis IoT dengan *QR Code*
Nama Mahasiswa	: Riski Arasyid
NIM	: H1051211025
Jurusan/Program Studi	: Rekayasa Sistem Komputer
Tanggal Lulus	: 25 Juli 2025
SK Pembimbing	: No. 263/UN22.8/TD.06/2025/Tanggal 03 Februari 2025
SK Penguji	: No. 2338/UN22.8/TD.06/2025/Tanggal 18 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.	Hafiz Muhardi, S.T., M.Kom.
NIP. 198607012014041001	NIP. 199007232023211017

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	: Riski Arasyid
NIM	: H1051211025
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



Riski Arasyid
NIM. H1051211025

Implementasi Kriptografi Vigenere Cipher untuk Keamanan Pengiriman Data pada Sistem *Smart Door* Berbasis *QR Code*

Abstrak

Sistem *Smart Door* berbasis Internet of Things (IoT) dengan QR Code menyediakan akses otomatis namun memiliki celah keamanan berupa potensi penyadapan data (*sniffing*). Penelitian ini mengimplementasikan algoritma Vigenère Cipher untuk mengenkripsi data yang dikirimkan, serta menganalisis ketahanan *ciphertext* terhadap serangan dan dampaknya terhadap waktu tunda (*delay*). Sistem dibangun menggunakan ESP32-CAM sebagai pemindai QR dan NodeMCU ESP32 sebagai pengendali utama, dengan enkripsi diterapkan pada tiga jalur komunikasi, ESP32-CAM ke server, server ke database, dan server ke ESP32. Pengujian dilakukan dengan melakukan *Sniffing*, analisis *delay*, serta evaluasi ketahanan *ciphertext* menggunakan tools dCode dan CryptoTool. Dari 20 hasil sniffing QR Code, 10 sampel diuji hanya 3 yang dikenali sebagai Vigenère Cipher oleh dCode, dan seluruhnya gagal didekripsi. Pada jalur server ke ESP32, hanya 1 dari 10 data yang terdeteksi dan tidak ada yang berhasil dipecahkan. Rata-rata *delay* sistem adalah 2,473 detik (pembukaan pintu) dan 3,491 detik (aktivasi *buzzer*), dengan beberapa deviasi akibat kestabilan jaringan. Hasil menunjukkan bahwa implementasi Vigenère Cipher mampu meningkatkan ketahanan komunikasi data terhadap serangan penyadapan, sehingga sesuai untuk perangkat IoT dengan keterbatasan sumber daya. Namun, diperlukan optimalisasi pada aspek *delay* agar sistem dapat memenuhi karakteristik *real-time* secara konsisten.

Kata Kunci: *Smart Door,* IoT*, QR Code,* Vigenere Cipher*,* Keamanan Data*, Sniffing, Delay.*

Implementation of Vigenere Cipher Cryptography for Data Transmission Security in QR Code-Based Smart Door Systems

Abstract

The Smart Door system based on the Internet of Things (IoT) using QR Code offers automated access but remains vulnerable to data sniffing attacks. This study implements the Vigenère Cipher algorithm to encrypt transmitted data and analyzes the ciphertext's resistance to attacks as well as its impact on communication delay. The system is built using ESP32-CAM as the QR scanner and NodeMCU ESP32 as the main controller, with encryption applied across three communication paths: ESP32-CAM to server, server to database, and server to ESP32. Testing involved data sniffing, delay analysis, and ciphertext evaluation using tools such as dCode and CryptoTool. From 20 sniffed QR Code results, 10 random samples were tested, and only 3 were recognized as Vigenère Cipher and none were decrypted successfully. In the server-to-ESP32 path, only 1 out of 10 ciphertexts was detected and all remained undeciphered. The average delay was recorded at 2.473 seconds (door unlocking) and 3.491 seconds (buzzer activation), with variations due to network stability. The results indicate that Vigenère Cipher effectively enhances data security in resource-constrained IoT devices, although delay optimization is needed to meet real-time system requirements.

***Keywords**: Smart Door, IoT, QR Code, Vigenere Cipher, Data Security, Sniffing, Delay.*

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 Vigenere Cipher untuk Keamanan Pengiriman Data pada Sistem *Smart Door* Berbasis *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. Kepada orang tua yang selalu memberikan dukungan, doa, motivasi, dan kasih sayang tanpa henti sepanjang perjalanan penulisan tugas akhir ini.
2. Bapak Prof. Dr. Gusrizal, S.Si., M.Si., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.
3. Bapak Tedy Rismawan , S.Kom., M.Cs., selaku Ketua Jurusan Rekayasa Sistem Komputer FMIPA Universitas Tanjungpura Pontianak sekaligus sebagai dosen Pembimbing Akademik (PA) yang telah memberi masukan dan motivasi yang membangun selama masa perkuliahan.
4. 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.
5. 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.
6. 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.
7. Bapak Hafiz Muhardi, S.T., M.Kom., selaku dosen Penguji Kedua, yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.

8. Kepada Bapak dan Ibu dosen yang telah membimbing dan memberikan ilmunya kepada saya selama menjadi mahasiswa di prodi Rekayasa Sistem Komputer ini.
9. Kepada saudara Muhammad Dito Asrofa, teman seperjuangan yang membantu banyak untuk menyelesaikan skripsi ini.
10. Kepada saudara Faishal Hady, sepuh dengan ide briliannya saat merasa stuck menghadapi permasalahan saat pengerjaan skripsi ini.
11. Pada 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, 25 Juli 2025



Riski Arasyid

DAFTAR ISI

LEMBAR PENGESAHAN ii
PERNYATAAN INTEGRITAS AKADEMIK iii
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* 9
2.3 Kriptografi 9
2.4 Kriptografi Vigenere Cipher 10
2.5 NodeMCU ESP32 11
2.6 ESP32-CAM 11
2.7 Arduino IDE 12
2.8 Modul *Relay* 12
2.9 *Solenoid Door lock* 13
2.10 *Buzzer* 13
2.11 *Cloud Server* 14
2.12 *Flowchart* 14
2.13 Laravel 15

2.14 *Delay* 15
2.15 UUID (*Universal Unique Identifier*) 16
2.16 Balsamiq Mockup 16
2.17 *Sniffing* 16
2.18 Kali Linux 17
2.19 Wireshark 17
2.20 Ettercap 18
2.21 Cryptool 18
2.22 dCode 19
BAB 3 METODE PENELITIAN 20
3.1 Studi Literatur 21
3.2 Analisis Kebutuhan 21
3.2.1 Kebutuhan Perangkat Keras 21
3.2.2 Kebutuhan Perangkat Lunak 21
3.3 Perancangan Sistem 21
3.3.1 Perancangan Perangkat Keras 22
3.3.2 Perancangan Perangkat Lunak 22
3.4 Implementasi 22
3.5 Pengujian 22
3.6 Data Hasil Pengujian 23
3.7 Kesimpulan dan Saran 23
BAB 4 PERANCANGAN 24
4.1 Deskripsi Sistem 24
4.2 Perancangan Arsitektur Sistem 26
4.3 Perancangan Perangkat Keras 29
4.4 Perancangan Perangkat Lunak 32
4.5 Perancangan Metode Vigenere Cipher 33
4.5.1 Proses Enkripsi 33
4.5.2 Proses Dekripsi 35
4.5.3 Proses Keseluruhan 36
4.6 Perancangan Basis Data 37
4.6.1 Tabel *Users* 38

4.6.2 Tabel Pengguna 38
4.6.3 Tabel qrcode_result 39
4.6.4 Tabel command_queues 40
4.7 Perancangan Antar Muka 40
4.7.1 Perancangan Antarmuka *Website Admin* 40
4.7.2 Perancangan antarmuka *Website User* 42
4.8 Perancangan Pengujian Metode dengan *Sniffing Attack* 43
4.9 Perancangan Pengujian Ketahanan Cipherteks 44
4.10 Perancangan Pengukuran *Delay* 45
BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN 46
5.1 Implementasi Perangkat Keras 46
5.2 Implementasi Perangkat Lunak 47
5.2.1 Tampilan Halaman Manajemen Pengguna 50
5.2.2 Tampilan Halaman Hasil Pembacaan *QR Code* 51
5.2.3 Tampilan Halaman *Log History* 51
5.2.4 Tampilan Halaman Dashboard Pengguna 52
5.3 Implementasi Metode Vigenere Cipher 53
5.3.1 Pengiriman Data UUID dari Server ke Website Pengguna 57
5.3.2 Pengiriman Hasil Pembacaan *QR Code* ke Server 59
5.3.3 Pengiriman Instruksi Autentikasi dari Server ke ESP32 60
5.4 Implementasi Pengujian 62
5.4.1 Pengujian Metode Vigenere Cipher 62
5.4.2 Pengujian Ketahanan Cipherteks 68
5.4.3 Pengujian Waktu *Delay* Sistem 72
5.5 Pembahasan 76
BAB 6 PENUTUP 79
6.1 Kesimpulan 79
6.2 Saran 79
DAFTAR PUSTAKA 81
LAMPIRAN 85

DAFTAR GAMBAR

Gambar 2. 1 NodeMCU ESP32 11
Gambar 2. 2 ESP32-CAM..... 11
Gambar 2. 3 Arduino IDE..... 12
Gambar 2. 4 Modul Relay..... 12
Gambar 2. 5 *Buzzer*..... 13
Gambar 4. 1 Ilustrasi Pengiriman Data Jalur Pertama 25
Gambar 4. 2 Ilustrasi Pengiriman Data Jalur Kedua..... 25
Gambar 4. 3 Ilustrasi Pengiriman Data Jalur Ketiga..... 26
Gambar 4. 4 Arsitektur Sistem *Smart Door*..... 28
Gambar 4. 5 Rancangan Keseluruhan Perangkat Keras..... 31
Gambar 4. 6 Diagram Alir Sistem *Smart Door*..... 33
Gambar 4. 7 Diagram Alir Proses Enkripsi 34
Gambar 4. 8 Proses Dekripsi..... 35
Gambar 4. 9 Proses Keseluruhan 37
Gambar 4. 10 Rancangan Tampilan Halaman Manajemen Pengguna..... 41
Gambar 4. 11 Rancangan Tampilan Halaman Hasil Pembacaan *QR Code*..... 41
Gambar 4. 12 Rancangan Tampilan Halaman *Log History*..... 42
Gambar 4. 13 Rancangan Halaman *Dashboard* Pengguna..... 42
Gambar 5. 1 Implementasi Perangkat Keras..... 47
Gambar 5. 2 Tampilan Halaman Manajemen Pengguna 50
Gambar 5. 3 Tampilan Halaman Pembacaan *QR Code*..... 51
Gambar 5. 4 Tampilan Halaman Log History..... 52
Gambar 5. 5 Tampilan Halaman Dashboard Pengguna..... 52
Gambar 5. 6 Waktu *Delay Selenoid* Terbuka..... 74
Gambar 5. 7 Waktu *Delay Buzzer* Berbunyi..... 75

DAFTAR TABEL

Tabel 2. 1 Perbandingan dengan Penelitian Terdahulu 7
Tabel 2. 2 Kategori *Delay* Jaringan standar TIPHON 15
Tabel 4. 1 Penggunaan Pin ESP32 dengan *relay* dan *buzzer* 31
Tabel 4. 2 Penggunaan Pin Relay dengan *Selenoid Door lock* dan Jack Female . 31
Tabel 4. 3 Penggunaan Pin *Selenoid Door lock* dengan Jack Female 32
Tabel 4. 4 Rancangan Tabel Users 38
Tabel 4. 5 Rancangan Tabel Pengguna 38
Tabel 4. 6 Rancangan Tabel qrcode_resul 39
Tabel 4. 7 Rancangan Tabel command_queues 40
Tabel 5. 1 Konversi Plainteks ke Indeks 53
Tabel 5. 2 Konversi Kunci ke Indeks Kunci 54
Tabel 5. 3 Penjumlahan dan Modulo 54
Tabel 5. 4 Konversi Balik ke Karakter 55
Tabel 5. 5 Konversi Cipherteks ke Indeks 55
Tabel 5. 6 Pengurangan dan Modulo 62 56
Tabel 5. 7 Konversi Balik ke Karakter(Dekripsi) 57
Tabel 5. 8 Pengujian Pengiriman Data Autentikasi 63
Tabel 5. 9 Pengujian Pengiriman Data *QR Code* 65
Tabel 5. 10 Pengujian Pengiriman Intruksi ESP32 67
Tabel 5.11 Pengujian Ketahanan Cipherteks *QR Code* 68
Tabel 5.12 Pengujian Ketahanan Cipherteks Intruksi 69
Tabel 5.13 Pengujian Brute Force Cipherteks *QR Code* 70
Tabel 5.14 Pengujian Waktu *Delay Selenoid* Terbuka 72
Tabel 5. 15 Pengujian Waktu *Delay Buzzer* Berbunyi 74

DAFTAR KODE PROGRAM

Kode Program 5. 1 Kode Program Pembacaan *QR Code* pada ESP32-CAM 47
Kode Program 5. 2 Kode Program Verifikasi UUID di Server 48
Kode Program 5. 3 Kode Program Mengambil Perintah dari Server 49
Kode Program 5. 4 Mengaktifkan Solenoid *Door lock* 50
Kode Program 5. 5 Mengaktifkan *Buzzer* 50
Kode Program 5. 6 Enkripsi UUID di Server 58
Kode Program 5. 7 Dekripsi UUID di Website Pengguna 58
Kode Program 5. 8 Enkripsi Hasil Pembacaan *QR Code* 59
Kode Program 5. 9 Dekripsi Hasil Pembacaan *QR Code* 60
Kode Program 5. 10 Enkripsi Perintah Intruksi 61
Kode Program 5. 11 Dekripsi Instruksi pada ESP32 61

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Teknologi *Internet of Things* (IoT) merupakan konsep yang menghubungkan objek fisik ke jaringan internet, sehingga memungkinkan objek-objek tersebut untuk saling berkomunikasi dan bertukar informasi. Data yang dihasilkan oleh objek fisik ini dapat dimanfaatkan untuk meningkatkan efisiensi, efektivitas, dan kenyamanan dalam kehidupan sehari-hari (Syahdi Nasution et al., 2023). IoT dapat diterapkan dalam berbagai bidang, salah satunya pada sistem *Smart Door lock*. *Smart lock* atau kunci pintu pintar merupakan sistem keamanan pintu dengan akses perangkat elektronik seperti ponsel, tablet, atau komputer yang terhubung dengan internet. Kunci pintu pintar ini memudahkan pengguna dalam membuka dan mengunci pintu rumah sehingga tidak harus menggunakan kunci fisik (Juniawan & Rismayana, 2024). Salah satu jenis *Smart Door* yang biasa digunakan adalah *Smart Door* berbasis *QR Code* yang digunakan sebagai alat autentikasi untuk membuka pintu. *QR Code (Quick Response Code)* adalah barcode dua dimensi yang dikembangkan oleh perusahaan Jepang Denso Wave pada tahun 1994. Keunggulannya terletak pada kemampuannya menyimpan informasi secara horizontal dan vertikal, sehingga mampu menampung data lebih banyak serta dapat dipindai dengan cepat (Rabbani, 2023). Dengan penerapan teknologi IoT pada sistem *Smart Door*, pemilik properti dapat memonitor dan mengontrol akses pintu secara realtime, meningkatkan keamanan, serta memberikan kenyamanan bagi penghuninya dengan mengatur kontrol akses yang lebih fleksibel dan efisien melalui aplikasi atau website.

Meskipun teknologi *Smart Door* berbasis *QR Code* ini dapat memberi kemudahan, namun teknologi ini memiliki tantangan berupa keamanan data, dimana terdapat ancaman dan serangan yang umum terjadi, seperti *Man-in-the-Middle* (MitM). Dalam skenario ini, penyerang dapat menyadap komunikasi antara aplikasi dan perangkat untuk mendapatkan akses tanpa izin (Lantz & Pierrou, 2022). Hal ini menjadi penting ketika analis keamanan menyadari bahwa sekitar

98% dari seluruh lalu lintas antar perangkat IoT tidak terenkripsi (Fereidouni et al., 2023). Salah satu jenis serangan *Man-in-the-Middle* (MitM) yang sering terjadi adalah *Sniffing*, yaitu teknik serangan yang dilakukan dengan memantau atau mengontrol setiap paket data yang dikirim melalui media komunikasi, baik kabel maupun nirkabel. Serangan ini dapat dilakukan melalui perangkat lunak atau perangkat keras khusus yang memonitor lalu lintas jaringan (Tamsir et al., 2024). Untuk mengatasi tantangan keamanan pada sistem *Smart Door* berbasis *QR Code*, dapat dilakukan penerapan teknologi kriptografi untuk melindungi integritas dan kerahasiaan data. Salah satu metode kriptografi yang bisa digunakan adalah Vigenère Cipher, yang dapat mengenkripsi data menggunakan kunci rahasia untuk memastikan keamanan komunikasi data pada sistem.

Selain aspek keamanan, penting juga untuk memperhatikan waktu *Delay* atau keterlambatan dalam proses autentikasi dan transmisi data. *Delay* yang tinggi dapat menyebabkan pengalaman pengguna yang buruk, terutama pada sistem yang dirancang untuk akses cepat seperti *Smart Door* berbasis *QR Code*. Oleh karena itu, pengukuran *Delay* dibutuhkan untuk mengevaluasi performa sistem secara menyeluruh, khususnya dalam konteks penerapan teknologi keamanan seperti kriptografi. Hasil penelitian menunjukkan bahwa pemilihan metode kriptografi yang digunakan dalam perangkat IoT berdampak signifikan terhadap peningkatan *Delay* dan panjang pesan tambahan. Hal ini menjadi penting bagi perangkat dengan sumber daya terbatas seperti ESP8266, ESP32, dan Raspberry Pi yang banyak digunakan pada sistem *smart home*, karena dapat memengaruhi efisiensi komunikasi antar perangkat. Dengan demikian, analisis terhadap *Delay* sangat diperlukan untuk menyeimbangkan aspek keamanan dan performa sistem secara optimal (Silva et al., 2024).

Dalam konteks penggunaan *Smart Door* berbasis *QR Code*, Vigenère Cipher dapat diterapkan untuk mengamankan data pada tiga jalur yaitu server ke website pengguna, ESP-CAM ke server, dan server ke ESP32. Data tersebut akan dienkripsi menggunakan kunci rahasia, sehingga hanya dapat dibaca oleh sistem yang memiliki kunci yang sama. Penerapan ini diharapkan membantu mengurangi risiko serangan seperti *Sniffing*, di mana peretas dapat mencoba menyadap data selama proses transmisi.

Penelitian sebelumnya yang berjudul "Sistem Keamanan Pintu Otomatis Berbasis *QR Code* dengan Teknologi IoT" (Basit et al., 2022) membahas tantangan dalam pengelolaan akses keamanan pintu pada perkantoran, dimana penggunaan kunci manual sering kali menyebabkan keterbatasan akses yang tidak efisien. Untuk mengatasi masalah ini, teknologi *Internet of Things* (IoT) menawarkan solusi melalui penerapan sistem *Smart Door* berbasis *QR Code*. Sistem ini menggunakan perangkat seperti Raspberry Pi, Pi Camera, dan modul *solenoid* yang terintegrasi dengan aplikasi berbasis *smartphone* untuk autentikasi pengguna. Dengan data autentikasi yang disimpan pada database berbasis web, sistem ini memungkinkan kontrol akses secara *real-time* dan hanya dapat diakses oleh pengguna yang terdaftar. Penelitian ini menunjukkan bahwa penggunaan teknologi *QR Code* pada sistem *Smart Door* dapat meningkatkan efisiensi dan keamanan akses, sekaligus memberikan kemudahan bagi pemilik properti dalam memonitor aktivitas pengguna secara akurat dan efisien.

Penelitian lain yang berjudul *"*Pengamanan Pesan Rahasia dengan Metode Vigenere Cipher Menggunakan PHP*"* (Murni et al., 2023) membahas implementasi metode Vigenère Cipher dalam mengamankan pesan teks berbasis web. Penelitian ini bertujuan untuk mengenkripsi pesan rahasia agar tidak dapat diakses oleh pihak yang tidak berwenang, dengan memanfaatkan bahasa pemrograman PHP sebagai media implementasi. Metode Vigenère digunakan karena kemampuannya melakukan substitusi abjad majemuk, di mana setiap karakter pada pesan digeser sesuai karakter kunci yang diberikan. Hasil enkripsi dan dekripsi diuji menggunakan file teks, serta divisualisasikan melalui *flowchart* untuk memperjelas proses kerja sistem. Penelitian ini menunjukkan bahwa metode Vigenère dapat diimplementasikan secara efektif dalam aplikasi web sederhana untuk meningkatkan keamanan informasi, khususnya pada transmisi pesan melalui internet.

Penelitian selanjutnya yang berjudul "*Testing Data Security Using a Vigenere Cipher Based on the QR Code*" (Rachmawanto et al., 2023) membahas tantangan dalam melindungi data yang disimpan dalam *QR Code* dari ancaman keamanan seperti manipulasi atau pencurian data. Penelitian ini menggunakan metode kriptografi Vigenère Cipher untuk mengenkripsi data sebelum dikonversi menjadi

QR Code. Proses enkripsi dilakukan dengan kunci rahasia untuk memastikan informasi yang tersimpan hanya dapat diakses oleh pihak yang memiliki kunci dekripsi. Hasilnya menunjukkan bahwa metode ini mampu meningkatkan keamanan data, sekaligus memungkinkan penggunaan *QR Code* sebagai media autentikasi yang efisien dan aman dalam berbagai aplikasi, termasuk sistem absensi dan verifikasi data secara daring.

Berdasarkan penelitian sebelumnya, maka diangkat sebuah penelitian yang berjudul "Implementasi Kriptografi Vigenère Cipher untuk Keamanan Pengiriman Data pada Sistem *Smart Door* Berbasis IoT dengan *QR Code*". Penelitian ini bertujuan untuk mengamankan data pada sistem *Smart Door* berbasis *QR Code*, di mana data tersebut dienkripsi menggunakan metode Vigenère Cipher sebelum dikirimkan dalam bentuk *ciphertext* (pesan rahasia). Proses ini memungkinkan hanya pihak yang berwenang dengan kunci dekripsi yang dapat mengakses data tersebut. Dengan penerapan ini, diharapkan sistem dapat mencegah ancaman keamanan seperti manipulasi data atau akses tidak sah dari pihak ketiga, sehingga meningkatkan keamanan dan keandalan sistem IoT berbasis *Smart Door*.

1.2 Rumusan Masalah

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

1. Bagaimana ketahanan ciphertext hasil enkripsi Vigenère Cipher terhadap serangan sniffing pada sistem Smart Door berbasis Internet of Things (IoT)?
2. Bagaimana pengaruh penggunaan Vigenere Cipher pada *QR Code* terhadap *Delay* dalam proses transmisi data pada sistem *Smart Door*?

1.3 Batasan Masalah

Batasan masalah penelitian ini adalah sebagai berikut:

1. Penelitian ini difokuskan pada pengembangan sistem *Smart Door* berbasis IoT yang menggunakan NodeMCU ESP32 sebagai perangkat utama.
2. Metode kriptografi yang digunakan adalah Vigenere Cipher, yang diterapkan pada pengiriman data di sistem *Smart Door*.

3. Evaluasi performa sistem dilakukan dengan mengukur *Delay* selama proses transmisi data mulai dari ESP32-CAM mengirim data pembacaan *QR Code* hingga ESP32 menjalankan perintah.
4. Data autentikasi berupa *QR Code* dihasilkan dan ditampilkan melalui website, tanpa melibatkan data biometrik atau data lain.
5. Penelitian ini tidak akan membahas keamanan pada infrastruktur server, tetapi hanya fokus pada keamanan di perangkat IoT *Smart Door*.
6. Jenis serangan yang diatasi adalah *Sniffing*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Meningkatkan ketahanan data terhadap sniffing dengan Vigenère Cipher pada sistem Smart Door IoT.
2. Mengetahui pengaruh penggunaan metode kriptografi Vigenere Cipher terhadap *Delay* pada Sistem *Smart Door* berbasis IoT dengan *QR Code*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah membantu menjaga keamanan data pada sistem *Smart Door*. Dengan penerapan metode kriptografi Vigenère Cipher, data pembacaan *QR Code* dan perintah yang dikirim dari perangkat pengguna ke sistem pintu pintar dapat dienkripsi, sehingga hanya pihak yang berwenang yang bisa mengakses informasi tersebut setelah proses dekripsi. Hal ini dapat mencegah serangan siber, seperti *Sniffing* dan *Man-in-the-Middle (MitM)*, dan memastikan keamanan serta integritas data selama transmisi.

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 data perangkat *Internet of Things*

(IoT) dan kenapa penelitian ini dilakukan, 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 kriptografi *Vigenere Cipher, NodeMCU ESP32, ESP32-CAM, Relay, Selenoid Door lock, Buzzer,* Arduino IDE ,Laravel.

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 *Smart Door* menggunakan NodeMCU ESP32 dan ESP32-CAM, dan perancangan keseluruhan perangkat keras. Sedangkan pada perancangan perangkat lunak meliputi perancangan sistem komunikasi antara NodeMCU ESP32 dan ESP32-CAM dengan *web server*, dan perancangan penerapan metode kriptografi Vigenere Cipher pada sistem *Smart Door* berbasis IoT dengan *QR Code*.

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.