BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telah berkembang secara pesat, terutama pada bidang robotika yang kini sudah mulai digunakan untuk membantu kehidupan sehari-hari dimasyarakat. Pada bidang robotika ini sendiri salah satu komunikasi yang dilakukan yaitu komunikasi serial dengan telemetri seperti tanpa kabel contohnya untuk melakukan pengukuran jarak jauh pada pemantauan suhu gunung berapi, gempa, tsunami, dan bencana alam lainnya ataupun dengan kabel untuk menggerakan suatu alat yang dipasangkan *microcontroller* salah satunya Arduino.

Komunikasi telemitri dengan serial merupakan sebuah sistem pengiriman dan penerimaan data yang didasari dari dengan cara komunikasinya yang memberikan 1-bit secara bergantian dalam satu waktu. Komunikasi ini biasa digunakan pada pengiriman data pada *microcontroller* yang banyak digunakan pada pemantauan secara telemetri. Tentu komunikasi seperti ini sangat sensitif karena permberian dan penerimaan informasinya yang dapat diserang ataupun dirusak oleh seseorang yang tidak bertanggung jawab. Oleh karena itu diperlukannya pengamanan dalam pengiriman dan penerimaan data untuk memberikan nilai keaslian dan kebenarannya.

Pengamanan data atau Kriptografi merupakan suatu teknologi yang digunakan untuk menjamin keamanan dan keutuhan dari informasi yang dikirim dan diterima. Dalam perkembangannya algoritma Kriptografi yang saat ini banyak digunakan yaitu Rijndael dan Twofish.

Algoritma Rijndael merupakan pemenang dari kontes kriptografi pengganti *Data Encryption Standard* (DES), yang dilakukan oleh *National Institutes of Standards and Technology* (NIST) milik pemerintah Amerika Serikat pada 26 November 2001, Rijndael inilah yang kemudian dikenal dengan *Advanced Encryption Standard* (AES). Setelah mengalami beberapa proses standardisasi oleh

NIST, Rijndael kemudian diadopsi menjadi standar algoritma secara resmi pada 22 Mei 2002. Pada 2006 AES merupakan salah satu algoritma kriptografi terpopuler yang digunakan dalam kriptografi kunci simetrik (Emy Setyaningsih, 2015).

Twofish merupakan algoritma kriptografi yang dikembangkan dari algoritma Blowfish mengikuti kriteria-kriteria kompetisi AES milik NIST seperti Rijndael, namun algoritma ini tidak terpilih sebagai basis untuk standardisasi tetapi masih banyak digunakan untuk melakukan pengamanan data.

Dengan perkembangan teknologi pada bidang robotika keamanan berkomunikasi pada sistem telemetri membutuhkan keamanan untuk memberikan nilai keaslian dan kebenaran data yang dikirim dan diterima dengan menggunakan algoritma-algoritma Kriptografi contohnya Rijndael dan Twofish .

Berdasarkan latar belakang permasalahan diatas, maka penulis mengambil judul **"ANALISIS PENGAMANAN DATA TELEMETRI DENGAN ALGORITMA RIJNDAEL DAN TWOFISH PADA SISTEM KOMUNIKASI SERIAL".**

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, peneliti merumuskan masalah yang diteliti dan dianalisa dalam bentuk pertanyaan penelitian sebagai berikut:

a. Bagaimana cara membangun sebuah sistem komunikasi dengan menggunakan pengamanan Rijndael dan Twofish?
b. Bagaimana menganalisa dan memilih algoritma yang lebih baik dalam sebuah sistem komunikasi serial?

1.3 Ruang Lingkup

Adapun ruang lingkup pembahasan yang akan dibahas dengan batasan sebagai berikut :

a. Dilakukan analisa pada algoritma Rijndael dan Twofish dengan data yang didapat dari PT. Transdata Global Solutions tempat penulis melakukan riset terkait tugas akhir.

b. Analisa dilakukan pada beberapa program pembantu yaitu Visual Basic dan Dev-C++ dan diujikan pada sistem telemetri kepada *microcontroller* Arduino.
c. Sistem yang diuji coba pada alat peraga yang dibangun oleh penulis dengan menggunakan Arduino dan beberapa alat pembantu.
d. Pengujian dilakukan menggunakan data masukan (*input/plaintext*).

1.4 Tujuan Penelitian

Tujuan penelitian yang ingin dicapai penulis dalam pelaksanaan tugas akhir ini adalah:

a. Mempelajari teknologi kriptografi data khususnya pada Rijndael dan Twofish.
b. Menganalisa algoritma Rijndael dan Twofish.
c. Mengetahui konsep, arsitektur, dan proses-proses enkripsi dan dekripsi khususnya pada kedua algoritma tersebut.
d. Memadukan konsep jaringan telemetri dengan keamanan data pada bangun sistem *microcontroller*.
e. Mengetahui kemungkinan kemampuan kedua algoritma pada sistem yang dibangun.

1.5 Manfaat Penelitian

Sesuai dengan permasalahan dan tujuan penelitian yang telah disebutkan diatas, maka manfaat penelitian dapat dirumuskan sebagai berikut:

a. Bagi Penulis

   Menambah pengetahuan dan meningkatkan keahlian penulis dalam merancang model kriptografi menggunakan algoritma Rijndael dan Twofish dalam sistem jaringan telemetri pada alat indentik yang digunakan yaitu alat komunikasi serial pada *microcontroller*.
b. Bagi Ilmu Pengetahuan dan Teknologi (IPTEK)

   Penelitian ini dapat dijadikan sebagai bahan pertimbangan atau dikembangkan lebih lanjut, serta juga sebagai referensi terhadap

penganalisaan penelitian yang berisikan kriptografi Rijndael dan Twofish dalam pengamanan data telemetri pada komunikasi serial.

c. Bagi Perusahaan

Memberikan keamanan dalam penyampaian data sebagai bentuk peningkatan keaslian dan keutuhan data yang diterima terutama kepada perusahaan yang bergerak dibidang telekomunikasi dan robotika.

1.6 Sistematika Penulisan

Adapun sistematika penulisan dari skripsi ini terdiri dari beberapa bagian utama sebagai berikut:

BAB 1 PENDAHULUAN

Pada bab ini berisikan latar belakang yang menjelaskan dasar dari penelitian ini, rumusan masalah, ruang lingkup, tujuan penelitian, manfaat penelitian, dan sistematika penulisan yang digunakan dalam penulisan ini.

BAB 2 TINJAUAN PUSTAKA

Pada bab ini berisi uraian teori-teori yang mendasari penelitian secara detail, dapat berupa metode, model, algoritma, teknik, konsep, prosedur, atau definisi yang berkaitan dengan topik penelitian.

BAB 3 METODOLOGI PENELITIAN

Pada bab ini menjelaskan tahapan penelitian atau kerangka pikir, dekripsi pendekatan tahapan penelitian, metode pengembangan, rancangan alur program, komponen *hardware* dan *software*, tempat dan jadwal penelitian yang digunakan untuk mencapai tujuan penelitian.

BAB 4 HASIL DAN PEMBAHASAN

Pada bab ini berisikan tentang implementasi program seperti uji coba program, dan penerapan serta analisa pengamanan data telemetri dalam sistem yang dibangun.

BAB 5 PENUTUP

Pada bab ini berisikan kesimpulan dan saran dari analisa algoritma yang dilakukan pada pengamanan data serial dalam sistem telemitri.

DAFTAR PUSTAKA

LAMPIRAN