BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan pesatnya perkembangan teknologi di era digital, distribusi perangkat lunak telah menjadi bagian tak terpisahkan dari kebutuhan komputasi modern. Namun, kemudahan dalam memperoleh dan menyebarkan aplikasi ini diiringi dengan meningkatnya ancaman keamanan *siber* yang semakin kompleks.

Salah satu jenis *malware* yang banyak digunakan oleh peretas adalah *Trojan* horse, yaitu perangkat lunak berbahaya yang menyamar sebagai aplikasi sah untuk mengecoh pengguna. *Trojan* sering kali disisipkan ke dalam *file installer (.exe),* aplikasi bajakan, atau dikirim melalui lampiran *email*. *Trojan* umumnya ditemukan dalam perangkat lunak bajakan *(pirated software)* yang telah dimodifikasi dan disusupi kode berbahaya. *Trojan* bekerja dengan cara menginfeksi sistem dan memberikan akses tidak sah kepada penyerang, sering kali tanpa sepengetahuan korban. Deteksi *Trojan* dapat dilakukan melalui metode *hybrid analysis*, yang mencakup analisis statis (*file* tanpa dijalankan) dan analisis dinamis (mengamati perilaku saat dijalankan dalam sistem) untuk mengidentifikasi aktivitas berbahaya secara menyeluruh (Damanik, Seta, & Theresiawati, 2023). Teknik ini terbukti efektif untuk memetakan pola serangan, seperti koneksi ke server command and control (C2), injeksi proses, serta aktivitas penyusupan data. Dengan demikian,

penggunaan hybrid analysis sangat relevan dalam upaya deteksi dan pencegahan penyebaran *Trojan* dalam sistem komputer.

Berdasarkan permasalahan tersebut, diperlukan sebuah sistem yang dapat menjamin keamanan *file installer (.exe)* sebelum didistribusikan. Kriptografi menawarkan solusi yang kuat untuk melindungi konten dari modifikasi dan akses tidak sah. Penelitian ini mengusulkan implementasi sebuah sistem keamanan *file installer (.exe)* menggunakan algoritma kriptografi RC4. Algoritma RC4 dipilih karena kinerjanya yang cepat sebagai *stream cipher*, sementara bahasa pemrograman Python digunakan karena fleksibilitas dan dukungannya yang luas terhadap pengembangan aplikasi keamanan.

Kriptografi awalnya didefinisikan sebagai ilmu yang mempelajari cara menyembunyikan pesan. Namun, dalam pengertian modern kriptografi adalah ilmu yang didasarkan pada teknik matematika untuk menangani keamanan informasi, termasuk kerahasiaan, keutuhan data dan otentikasi entitas (R. Fauzi, 2023). Enkripsi ini mengubah data asli *(plaintext)* menjadi kode yang hanya bisa diubah kembali ke bentuk aslinya *(ciphertext)* oleh pihak yang memiliki kunci dekripsi yang tepat. Salah satu algoritma kriptografi yang sering digunakan adalah RC4, sebuah stream cipher yang dirancang oleh Ron Rivest pada tahun 1987. RC4 bekerja dengan menggunakan kunci simetris untuk menghasilkan *keystream* yang digunakan untuk mengenkripsi *plaintext* melalui operasi *XOR* sederhana.

Algoritma RC4 *(Ron's Code / Rivest's Cipher)* adalah salah satu algoritma yang dapat digunakan untuk melakukan enkripsi data sehingga data asli hanya dapat dibaca oleh seseorang yang memiliki kunci enkripsi tersebut. Contoh yang dibahas kali ini adalah mengenai enkripsi dan dekripsi dari sebuah kalimat. Algoritma ini merupakan pengembangan dari RC2 dan dikembangkan oleh penemu algoritma tersebut, yaitu Ronald Rivest. Rivest code 4 (RC4) adalah perhitungan kriptografi kunci simetris canggih yang memiliki mode kerja stream chipper, sehingga dalam menangani informasi dan data pada waktu tertentu menggunakan dua kotak pengganti (s-box) sebagai tampilan dengan panjang perubahan 256 dan selanjutnya s-box kedua yang merupakan elemen dari perhitungan public key. Rivest Code 4 digunakan untuk menyandikan informasi, pesan atau data.*(Arifah, Tahir, Fadli, Nafasa, Zahrah & Rohmah, 2023).*

Python merupakan sebuah bahasa pemrograman interpretatif yang memiliki banyak fungsi, dan didesain dengan fokus pada kejelasan dan kemudahan pemahaman kode. *Python* dianggap sebagai bahasa yang menggabungkan kemampuan dan kejelasan sintaks kode. Bahasa pemrograman *Python* dirancang khusus untuk memudahkan programmer dalam membuat program dengan efisiensi waktu, kemudahan pengembangan, dan kompatibilitas dengan sistem. *Python* dapat digunakan untuk membuat aplikasi mandiri atau pemrograman skrip (Aqmila, 2022). Python adalah sebuah bahasa pemrograman berbasis objek yang dapat diinteraksi secara interaktif (Ridho, & Niani, 2

1.2 Rumusan Masalah

1. Bagaimana mengimplementasikan sebuah sistem aplikasi untuk enkripsi dan dekripsi *file installer (.exe)* dengan menerapkan algoritma kriptografi RC4 menggunakan bahasa pemrograman Python?
2. Bagaimana menguji kinerja sistem yang dibangun dalam hal kecepatan proses enkripsi-dekripsi serta keberhasilan dalam menjaga keutuhan *file*?

1.3 Batasan Masalah

Agar pembahasan lebih terarah dan sesuai dengan judul Tugas Skripsi yang telah ditentukan, penulis hanya membahas pokok – pokok bahasan sebagai berikut:

1. Penelitian ini hanya membahas implementasi algoritma RC4 untuk proses enkripsi dan dekripsi *file installer (.exe)*
2. Pengujian dilakukan dalam lingkungan sistem operasi Windows, baik versi 32-bit maupun 64-bit. Platform lain seperti Linux atau macOS tidak menjadi cakupan pengujian utama.
3. Implementasi algoritma dan pengembangan aplikasi dilakukan menggunakan bahasa pemrograman Python dengan pustaka pendukung seperti Tkinter, PyCryptodome, OS, secrets, threading, dan datetime

1.4 Tujuan dan Manfaat

1.4.1 Tujuan Penelitian

1. Merancang dan membangun sebuah sistem aplikasi untuk mengamankan *file installer (.exe)* dengan menerapkan algoritma kriptografi RC4.
2. Mengimplementasikan proses enkripsi untuk melindungi konten *file installer (.exe)* dari ancaman modifikasi tidak sah dan potensi penyisipan *malware* seperti *Trojan*.
3. Menguji dan menganalisis kinerja sistem yang telah dibangun, khususnya dalam hal kecepatan proses enkripsi dan keberhasilan dalam menjaga keutuhan data.

1.4.2 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Mengimplementasikan algoritma RC4 untuk melindungi *file installer (.exe)* dari ancaman modifikasi tidak sah dan penyisipan *malware* seperti *Trojan.*
2. Menambah wawasan dan referensi ilmiah mengenai penerapan algoritma RC4 dalam konteks pengamanan *file* digital, khususnya *file installer* (.exe).

1.5 Metodologi Penelitian

Berikut adalah langkah-langkah metodologinya:

1. Studi Kepustakaan

   Mengkaji dasar teori mengenai algoritma kriptografi RC4. Selanjutnya, menganalisis kebutuhan fungsional untuk menentukan fitur-fitur utama sistem.

2. Perancangan Sistem

   Mendesain arsitektur dan alur kerja aplikasi, termasuk proses enkripsi dan dekripsi. Kemudian, merancang tata letak antarmuka pengguna (UI) agar mudah dioperasikan.

3. Implementasi Sistem

   Menerjemahkan hasil perancangan ke dalam kode program fungsional menggunakan Python. Proses ini memanfaatkan pustaka Tkinter, PyCryptodome, OS, secrets, threading, datetime.

4. Pengujian Aplikasi

   Melakukan pengujian fungsionalitas dengan metode *black-box* pada aplikasi yang telah dibuat. Pengujian ini bertujuan untuk memverifikasi bahwa setiap fitur berjalan tanpa kesalahan.

5. Penyusunan Laporan

   Menyusun seluruh proses dan hasil penelitian ke dalam format laporan tugas akhir. Terakhir, menarik kesimpulan berdasarkan analisis hasil pengujian yang telah dilakukan.

1.6 Sistematika Penulisan

Sistematika penulisan Tugas Skripsi ini dibagi atas beberapa bab, dimana masing-masing bab dibagi atas beberapa bab sub agar mempermudah penjelasan mengenai penelitian yang dilakukan dan mempermudah pembaca dalam memahami isi penelitian. Adapun sistematika penulisan Tugas Skripsi ini adalah sebagai berikut:

BAB 1 PENDAHULUAN

Pendahuluan berisi tentang Latar Belakang Masalah, Rumusan Masalah, Tujuan, Manfaat, Batasan Masalah, Metodologi Penlitian dan Sistematika Penulisan dalam pembuatan Tugas Skripsi.

BAB 2 TINJAUAN PUSTAKA

Bab ini membahas landasan teori yang menjadi dasar dalam penelitian. Pembahasan mencakup konsep keamanan informasi, kriptografi, serta algoritma RC4 secara mendalam sebagai metode utama dalam pengamanan data. Bab ini juga menguraikan teori mengenai *file installer(.exe)* sebagai objek penelitian serta teknologi pendukung seperti bahasa pemrograman Python.