BAB I
PENDAHULUAN

1.1 Latar Belakang

Berdasarkan laporan *monitoring* keamanan siber dari Badan Siber dan Sandi Negara (BSSN), mencatat bahwa telah terjadi 330.527.636 juta serangan siber terhadap Indonesia pada tahun 2024, dimana terdapat serangan yang mengeksploitasi kerentanan perangkat lunak untuk mendapatkan akses ke *server* dan mencuri data pengguna. *File source code* yang merupakan inti dari suatu sistem perangkat lunak memerlukan perlindungan ekstra untuk memastikan integritas dan kerahasiaannya. Kriptografi dapat menjadi solusi yang efektif dalam mengamankan data, dan penerapannya pada *file source code* dapat menjadi langkah yang signifikan dalam melindungi aset intelektual dan menjaga keberlanjutan pengembangan perangkat lunak. Di Indonesia terdapat undang-undang yang mengatur tentang perlindungan data pribadi, yaitu UU No 11 tahun 2008 tentang ITE pasal 26 ayat 1 yang menyatakan "penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan". Kemudian agama Islam juga secara tegas menetapkan betapa pentingnya untuk menjaga privasi setiap individu. Berikut ini adalah salah satu ayat dari Al-Qur'an yang mengisyaratkan untuk menjaga privasi, melalui firman Allah SWT yang tertulis didalam Al-Qur'an Surah An-Nur ayat 27 yang berbunyi :

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَأْنِسُوْا وَتُسَلِّمُوْا عَلٰٓى اَهْلِهَاۗ ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ

Menurut tafsiran Prof. Dr. Quraish Shihab, dalam bukunya yang berjudul Tafsir Al-Mishbah, "*Wahai orang-orang yang beriman, janganlah kalian memasuki rumah yang bukan milik kalian kecuali setelah meminta izin kepada penghuninya untuk memperkenankan kalian masuk setelah memberi salam*". Didalam bukunya beliau menegaskan, permintaan izin dan pemberian salam itu lebih baik bagi kalian ketimbang

masuk begitu saja, tanpa izin dan salam. Allah menentukan demikian agar kalian dapat mengambil pelajaran dan melaksanakannya (Shihab, 2021).

Pentingnya menjaga kerahasiaan dan integritas dari *file source code* tidak bisa diremehkan, mengingat risiko pencurian data, pelanggaran keamanan, penggunaan ilegal dan modifikasi tidak sah yang dapat merugikan seorang pengembang dan pemilik perangkat lunak. *File source code* tidak hanya mencakup instruksi untuk menjalankan program, tetapi juga mengandung informasi sensitif seperti algoritma, logika bisnis, dan desain aplikasi yang merupakan aset berharga bagi seorang pengembang dan suatu organisasi perusahaan.

Pada penelitan ini akan mengimplementasikan algoritma *Base64*, *Beaufort Cipher* dan *Vigenere Cipher* untuk pengamanan *file source code* bahasa pemrograman. Algoritma *Beaufort Cipher* dan *Vigenere Cipher* merupakan algoritma kriptografi klasik telah lama dikenal dan digunakan dalam berbagai konteks. Kemudian algoritma *Beaufort Cipher* dan *Vigenere Cipher* termasuk kedalam tipe algoritma simetris, yang artinya menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, atau disebut juga dengan (*single-key algorithm*). Penerapan kriptografi yang digunakan untuk pengamanan *file source code* bahasa pemrograman masih belum sepenuhnya dieksplorasi. Penggunaan algoritma *Base64* dan dua algoritma kriptografi secara bersamaan, dapat memberikan tingkat keamanan yang tinggi dan kompleks. Mengapa menggunakan algoritma *Beaufort Cipher* dan *Vigenere Cipher*, karena algoritma tipe simetris memiliki kelebihan seperti, kecepatan operasi komputasi yang tinggi karena algoritma ini dirancang sehingga proses enkripsi dan dekripsi membutuhkan waktu yang singkat maka cocok digunakan untuk sistem *real-time encription*, kemudian dapat menggunakan kunci relatif lebih pendek.

Jika pada penelitian terdahulu yang dilakukan oleh (Rachmadsyah et al., 2020) dan (Setiadi et al., 2020) menggunakan algoritma serupa untuk pengamanan pesan teks berbasis *mobile application* dan untuk pengamanan citra digital *grayscale*, maka pada penelitian ini diterapkan untuk pengamanan isi dari *file source code* bahasa pemrograman. Kemudian pada penelitian yang dilakukan oleh (Rangga, 2022) yang melakukan modifikasi algoritma *Beaufort Cipher* dengan transposisi grup simetri, maka pada penelitian ini melakukan sedikit modifikasi pada rumus algoritma *Beaufort*

Cipher dan *Vigenere Cipher* agar dapat disandingkan dengan algoritma *Base64*, yang memiliki jumlah 64 karakter.

Pembaruan yang dilakukan dalam penelitian ini adalah terletak pada konsep dan algoritma yang digunakan untuk pengamanan isi dari *file source code* bahasa pemrograman, dan algoritma *Beaufort Cipher* dan *Vigenere Cipher* yang sedikit dimodifikasi agar dapat disandingkan dengan algoritma *Base64*, agar terhindar dari karakter spesial yang tidak dapat terikut dalam proses enkripsi. Urgensi menggunakan dua algoritma kriptografi yaitu untuk peningkatan keamanan dan mengurangi risiko serangan terhadap satu algoritma.

Berdasarkan uraian yang dikemukakan diatas, maka penulis ingin mengangkat topik tugas akhir dengan judul penelitian "Implementasi *Base64*, *Beaufort Cipher*, *Vigenere Cipher* Untuk Pengamanan *File Source Code* Dalam Bahasa Pemrograman".

1.2 Rumusan Masalah

Mengacu pada latar belakang diatas, maka secara keseluruhan permasalahan yang akan dibahas dalam penelitian ini adalah sebagai berikut :

1. Bagaimana mengimplementasikan algoritma *Base64*, *Beaufort Cipher* dan *Vigenere Cipher* untuk pengamanan *file source code*?
2. Bagaimana proses enkripsi dan dekripsi *file source code* dengan mengimplementasikan algoritma *Base64*, *Beaufort Cipher*, *Vigenere Cipher*?
3. Bagaimana membangun aplikasi dalam mengamankan *file source code* dengan mengimplementasikan algoritma *Base64*, *Beaufort Cipher*, *Vigenere Cipher*?

1.3 Batasan Masalah

Pada saat melakukan penelitian ini, terdapat batasan ruang lingkup masalah yang sedang diteliti. Batasan-batasan masalah yang digunakan yaitu :

1. Penelitian ini berfokus untuk melakukan pengamanan isi dari *file source code* dalam berbagai ekstensi bahasa pemrograman, serta hanya mengenkripsi berbasis teks (*string*).
2. Algoritma kriptografi yang digunakan yaitu algoritma *Beaufort Cipher* dan *Vigenere Cipher*, menggunakan jenis kunci yang simetris.

3. Proses enkripsi dan dekripsi algoritma *Beaufort Cipher* dan *Vigenere Cipher*, menggunakan penyandian karakter *Base64*, yang terdiri dari 64, dengan sedikit memodifikasi dibagian rumus algoritma kriptografi menjadi *modulo* 64, dan hanya menggunakan kunci dengan karakter *Base64 alphabet*.

1.4 Tujuan Penelitian

Mengacu pada latar belakang diatas, maka tujuan dari penelitian ini adalah sebagai berikut :

1. Untuk mengetahui bagaimana proses enkripsi dan dekripsi pada *file source code* bahasa pemrograman dengan mengimplementasikan algoritma *Base64*, *Beaufort Cipher* dan *Vigenere Cipher*.
2. Untuk menerapkan algoritma *Base64*, *Beaufort Cipher* dan *Vigenere Cipher* dalam mengamankan *file source code* bahasa pemrograman.
3. Untuk membangun aplikasi dalam mengamankan *file source code* bahasa pemrograman dengan mengimplementasikan algoritma *Base64*, *Beaufort Cipher* dan *Vigenere Cipher*.

1.5 Manfaat Penelitian

Hasil dari penelitian ini, harapannya dapat memberikan manfaat. Berikut adalah beberapa manfaat yang diharapkan dari penelitian ini :

1. Penelitian ini menghasilkan aplikasi berbasis *web* yang bertujuan untuk memfasilitasi seorang pengembang aplikasi yang ingin menjaga kerahasiaan dari isi *file source code*. Aplikasi ini mencapai tujuannya yaitu mengimplementasikan algoritma *Base64*, *Beaufort Cipher*, *Vigenere Cipher*.
2. Penelitian ini memberikan pengetahuan dan pemahaman tentang proses pengamanan *file source code* bahasa pemrograman, menggunakan algoritma *Base64*, *Beaufort Cipher* dan *Vigenere Cipher*.
3. Penelitian ini memberikan metode praktis penerapan kriptografi pada lingkungan pengembangan perangkat lunak, dan dapat menjadi landasan bagi praktisi keamanan perangkat lunak untuk meningkatkan keamanan *file source code* mereka.