**LAPORAN**

**STUDI KASUS**

**MATEMATIKA DISKRIT**

**“ Program Enkripsi dan Dekripsi Kuantum Caesar Cipher (QCC) v1.0 ”**



Disusun Oleh:

|  |  |
| --- | --- |
| Nama | : Reyhanssan Islamey |
| NIM | : 2200018411 |
| Kelas | : A |
| Slot | : Selasa 12.00 |

**LABORATORIUM KOMPUTER INFORMATIKA**

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS TEKNOLOGI INDUSTRI**

**UNIVERSITAS AHMAD DAHLAN**

**YOGYAKARTA**

**2023**

1. **DESKRIPSI STUDI KASUS**

Caesar Cipher adalah salah satu jenis cipher yang paling sederhana dalam dunia kriptografi. Cara kerja Caesar Cipher adalah dengan menggeser setiap huruf dalam plaintext sejauh n karakter (dalam contoh ini, n adalah jumlah pergeseran yang ditentukan). Sebagai contoh, huruf A akan diganti dengan huruf B apabila jumlah pergeseran n adalah 1. Namun, Caesar Cipher memiliki kelemahan yang besar, yaitu mudah untuk didekripsi dengan melakukan brute force pada setiap kemungkinan pergeseran.

Dalam upaya untuk meningkatkan keamanan Caesar Cipher, terdapat suatu metode baru yang menggunakan Quantum Computing sebagai alat untuk melakukan enkripsi dan dekripsi pesan. Metode tersebut menggunakan konsep superposisi dan entanglement dari partikel sub-atomik untuk membuat pesan tersebut menjadi aman dari serangan brute force.

Maka dari itu, dalam studi kasus ini kita akan mempelajari cara implementasi Caesar Cipher pada Quantum Computing menggunakan bahasa pemrograman Python dan library Qiskit. Dalam studi kasus ini, kita akan menggunakan materi yang telah dipelajari pada pertemuan sebelumnya dan menerapkannya pada kasus yang lebih mendalam.

Dalam kehidupan sehari-hari, kita sering kali membutuhkan suatu bentuk komunikasi yang aman dan terenkripsi. Kita dapat mengirim pesan-pesan rahasia melalui email, pesan teks, atau bahkan media sosial. Namun, kita seringkali khawatir bahwa pesan tersebut akan dibaca oleh orang yang tidak berhak atau bahkan oleh pengguna jaringan yang tidak bertanggung jawab.

Itulah mengapa Caesar Cipher dengan Quantum Computing menjadi sangat penting. Metode ini mampu mengamankan pesan-pesan penting dengan cara yang lebih aman dan efektif dibandingkan dengan metode enkripsi klasik lainnya.

Dalam studi kasus ini, kita akan membahas bagaimana Caesar Cipher dengan Quantum Computing dapat membantu mengatasi masalah keamanan pesan di kehidupan sehari-hari. Kita dapat mengirim pesan-pesan rahasia dengan aman dan nyaman tanpa khawatir akan dibaca oleh orang yang tidak berhak.

Selain itu, implementasi Caesar Cipher pada Quantum Computing juga dapat digunakan dalam berbagai bidang, seperti keuangan, militer, dan bisnis. Dalam bidang keuangan, Caesar Cipher dengan Quantum Computing dapat membantu melindungi data keuangan dan informasi penting dari pencurian dan serangan cyber. Dalam bidang militer, teknologi ini dapat melindungi pesan-pesan rahasia dan strategi militer dari musuh.

Secara umum, implementasi Caesar Cipher pada Quantum Computing memiliki banyak manfaat dan kegunaan dalam kehidupan sehari-hari. Kita dapat mengatasi masalah keamanan pesan dan melindungi informasi penting dari serangan cyber dan pencurian. Penggunaan teknologi ini dapat membantu menjaga keamanan dan kerahasiaan data dalam berbagai bidang, dan menjadi solusi untuk masalah sehari-hari yang seringkali dihadapi oleh banyak orang.

Saya sendiri memutuskan untuk mengambil program ini karena saya sangat tertarik dengan kriptografi dan ingin mempelajari lebih dalam tentang teknologi Quantum Computing. Selain itu, saya juga menyadari bahwa keamanan data sangat penting dalam kehidupan sehari-hari, dan saya ingin berkontribusi untuk menciptakan solusi yang lebih aman dan efektif untuk masalah tersebut.