PENJELASAN

Dalam program Caesar Cipher saya, saya memilih untuk menggunakan kriptosistem simetris. Ini berarti bahwa kita menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi pesan. Dalam hal ini, kunci tersebut adalah nilai shift yang kita tentukan sendiri. Ada beberapa alasan mengapa saya memilih kriptosistem simetris:

1. **Mudah dan Cepat:** Kriptosistem simetris seperti Caesar Cipher sangat sederhana untuk dipahami dan diimplementasikan. Proses mengenkripsi dan mendekripsi pesan juga berlangsung lebih cepat dibandingkan dengan metode lain.
2. **Efisiensi:** Dengan menggunakan kunci yang sama untuk enkripsi dan dekripsi, kita bisa memproses data lebih efisien. Ini sangat berguna jika kita ingin mengamankan banyak pesan dengan cepat.
3. **Kunci yang Mudah Diingat:** Kunci dalam sistem ini biasanya berupa angka yang tidak terlalu kompleks, sehingga mudah diingat dan dikelola. Ini berbeda dengan beberapa sistem lain yang mungkin memerlukan kunci yang panjang dan rumit.
4. **Cocok untuk Komunikasi Antara Dua Pihak:** Jika kita berkomunikasi dengan seseorang yang sudah kita percayai, menggunakan kunci simetris sangat efektif. Kita bisa sepakat tentang kunci yang akan digunakan dan menjaga kerahasiaannya tanpa perlu khawatir tentang pengaturan yang rumit.

Kekurangan Kriptosistem Simetris:

Meskipun ada banyak keuntungan, ada juga kekurangan, seperti:

- **Distribusi Kunci:** Menjaga dan mendistribusikan kunci antara pihak-pihak yang berkomunikasi bisa menjadi tantangan. Jika kunci jatuh ke tangan yang salah, keamanan pesan dapat terancam.
- **Tidak Skalabel:** Dalam situasi dengan banyak pihak, kebutuhan untuk berbagi kunci secara individual dapat menjadi rumit dan tidak efisien.