

1. **Sebutkan komponen utama dalam sebuah kriptosistem**

* Plaintext : Merupakan pesan atau informasi asli yang ingin dijaga kerahasiaanya sebelum dienkripsi.
* Chipertext : Hasil dari proses enkripsi, berp\upa pesan yang telah diubah menjadi bentuk tidak terbaca.
* Algoritma Enkripsi : Metode atau prosedur yang digunakan untuk mengonversi plaintext menjadi chipertext dengan bantuan kunci tertentu.
* Algortima Deskripsi : Metode yang digunakan untuk mengembalikan chipertext ke bentuk semula (plaintext) menggunakan kunci yang sesuai.
* Kunci (Key) : Nilai rahasia yeng berperan penting dalam proses enkripsi dan deskripsikarena keamanan system sepenuhnya begrgantung pada kerahasiaan kunci ini.

1. **Apa kelebihan dan kelamahan system simetris dibandingkan asimetris?**

Sistem kriptografi simetris memiliki kelebihan yaitu proses enkripsi dan dekripsinya lebih cepat karena menggunakan satu kunci yang sama, algoritmanya sederhana sehingga efisien untuk mengenkripsi data dalam jumlah besar, serta membutuhkan sumber daya komputasi yang lebih sedikit.

Namun, sistem ini juga memiliki kelemahan, yaitu distribusi kunci menjadi masalah karena pengirim dan penerima harus memiliki kunci yang sama dan harus menjaganya tetap aman. Selain itu, keamanan sistem akan terganggu jika kunci diketahui oleh pihak lain, dan sistem ini kurang cocok digunakan untuk komunikasi terbuka karena sulit menjamin keamanan pertukaran kunci. Sebaliknya, sistem asimetris memang lebih aman dalam hal distribusi kunci karena menggunakan kunci publik dan privat, tetapi memiliki proses yang lebih lambat dan membutuhkan daya komputasi lebih tinggi.

1. **Mengapa distribusi kunci menjadi maslash utama dalam kriptografi simetris?** Distribusi kunci menjadi masalah utama dalam kriptografi simetris karena sistem ini menggunakan **satu kunci yang sama** untuk proses enkripsi dan dekripsi. Artinya, baik pengirim maupun penerima pesan harus memiliki kunci yang identik sebelum komunikasi dimulai. Tantangannya adalah bagaimana cara mengirimkan kunci tersebut dengan **aman**, agar tidak disadap atau dicuri oleh pihak yang tidak berwenang. Jika kunci berhasil diketahui oleh orang lain, maka seluruh pesan yang dienkripsi dapat dengan mudah dibuka, sehingga keamanan sistem menjadi tidak terjamin.