Kryptering

Formålene med kryptering

- **Fortrolighed:** Beskytter data mod uautoriseret adgang.
- **Integritet:** Sikrer, at data ikke ændres uden detektion.
- **Autenticitet:** Bekræfter identiteten af kommunikerende parter.
- **Tilgængelighed:** Garanterer, at data kan gendannes af autoriserede brugere.

Symmetrisk Kryptering

- **Beskrivelse:** Bruger én nøgle til både kryptering og dekryptering.
- **Fordele:** Hurtig og effektiv, især til store datamængder.
- **Ulemper:** Sikker deling af nøgle er kritisk.
- **Eksempler:** AES, DES.
- **Anvendelse:** Diskkryptering, netværksprotokoller som WPA2.

Asymmetrisk Kryptering

- **Beskrivelse:** Bruger et nøglepar: en offentlig nøgle til kryptering og en privat nøgle til dekryptering.
- **Fordele:** Løser nøgleudvekslingsproblemer, muliggør digitale signaturer.
- **Ulemper:** Langsommere og kræver mere computerkraft.
- **Eksempler:** RSA, ECC.
- **Anvendelse:** Sikker nøgleudveksling (TLS/SSL), digitale signaturer.

Kombination af Symmetrisk og Asymmetrisk Kryptering

Mange systemer bruger asymmetrisk kryptering til nøgleudveksling og derefter symmetrisk kryptering til selve datatransmissionen. Eksempel: HTTPS.

HTTPS og Kryptering

- **Hvordan det virker:** HTTPS kombinerer symmetrisk og asymmetrisk kryptering.
- **Sikkerhed:** Garanterer fortrolighed, autenticitet og integritet.