Datakom. - Time 2017-09-13

Sikker og usikker forbindelse.

En kommunikasjon mellom to datamaskiner kan være usikker. Det betyr at det er mulig å se hva som sendes, hvis du bryter deg inn på forbindelsen. Alt foregår i klartekst. Hvis du sender f.eks. brukernavn og passord på en usikker forbindelse, kan en tredjepart få tak i ditt brukernavn og passord.
Eksempler på usikre forbindelser: Terminalemuleringsprogrammet telnet og (den usikre versjonen av) FTP (File Transfer Protocol). Da alt foregår i klartekst ved bruk av disse programmene, bør man ikke bruke disse programmer.

Hvis en kommunikasjon mellom to datamaskiner er sikker, er all data (tekst og annet) kryptert. Da kan man ikke finne ut hva som er innholdet i det som sendes, uten å ha en «nøkkel» som brukes til dekryptering.
Eksempler på sikre forbindelser: Terminalemuleringsprogrammet SSH (Secure Shell) og filoverføringsprogrammet SCP (Secure Copy). Brukes disse, er innholdet i en pakke kryptert, og kan ikke leses uten å ha den riktige nøkkelen til dekryptering.

Kryptering vha nøkler.

I en sikker dataoverføring er dataene som sendes kodet (kryptert) slik at det er umulig å finne ut hva som egentlig er i dataene. Eneste måten du kan finne det ut på er å ha en nøkkel. Det finnes to typer nøkler: en public nøkkel, som du skal sende til de som skal sende noe kryptert tilbake til deg. For å dekode tilbake brukes en privat nøkkel. Innholdet i den må ikke komme på avveie.

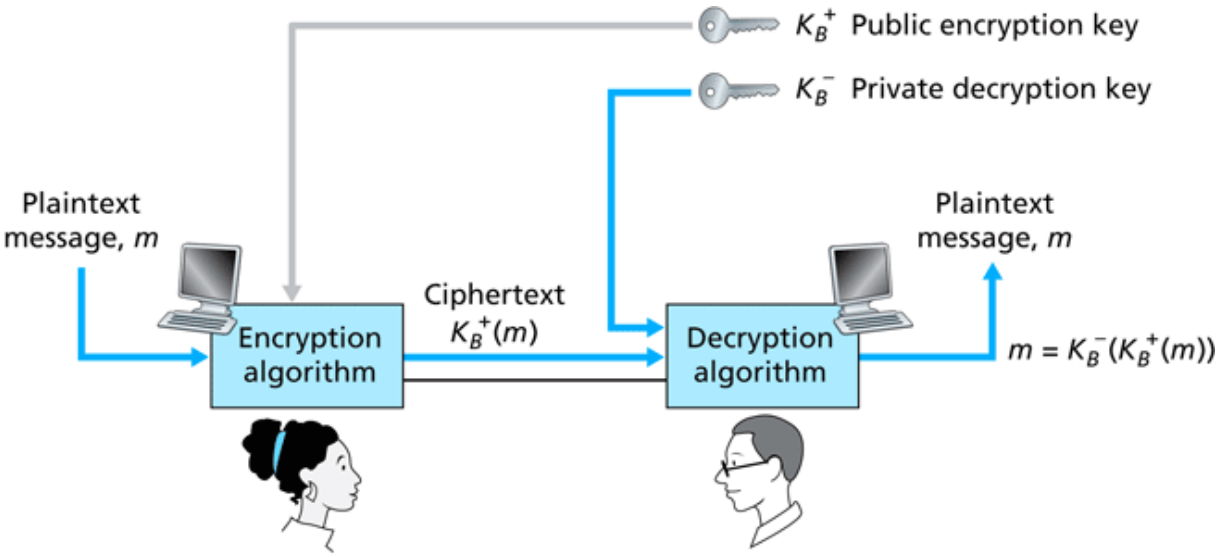

Figure 8.6 ♦ Public key cryptography