1 Sikkerhed

Behovet for sikkerhed, specielt med henblik på de to ting vi vil betragte:

Stikord: Fortrolighed, authentification, integritet, tilgængelighed.

1.1 Beskriv ideen i henholdsvis symmetrisk- og offentlig-nøgle kryptografi

Symmetrisk nøgle: En nøgle til at kryptere og dekryptere.

Asymmertisk nøgle/public key: En offentlig nøgle og en hemmelig nøgle.

Stikord: DES, RSA, public key, private key, (private)x(public) og (public)x(private) er ækvivalente.

1.2 Skitser protokoller for etablering af authentificerede forbindelser imellem Alice og Bob

Vil vise en, til gengæld en der virker `;-)`. Den bruger public key konceptet.

Stikord: "Jeg er alice", Bob onetime key, Alice private key, kryptering af onetime key, Bob bruger Alices public key.