11174 Datasikkerhet

Øving 6

1. Hva er en Kerberos ticket?

2. Tegn en figur, og forklar med egne ord meldingsflyten i Kerberos-protokollen når en bruker på en klient skal få tilgang til en tjeneste på en server. Kommenter spesielt bruken av sesjonsnøkler.

3. Et "utfordring-svar" (challenge-response) autentiseringssystem brukes i mange klassiske applikasjoner, og blir fremdeles brukt i mange sammenhenger. Meldingsflyten er som følger:

	A		B
Tid T_1		hallo→	
Tid T_2	←challenge		
Tid T_3		F_K(challenge)→	

   Resultatet av F_K(challenge) er det som omtaler som *response*. Sammenlign denne protokollen med Kerberos, og påpek de viktigste forskjellene/svakhetene