**ITGK ØVING 9-TEORI**

1. **Hvordan behandler TCP en tapt pakke (Lost packets)?**

Hver gang en pakke ankommer vil mottaker motta en bekreftelse, eller en ACK. Hver gang en pakke blir sendt vil TCP starte en timer. Dersom pakken ankommer før timeren utløper, vil timeren bli kansellert. Men dersom timeren utløper før pakken ankommer, vil det bli sendt en kopi av pakken og en ny timer starter. Dette kalles retransmisjon. Det er begrenset antall retransmisjoner som er mulig. Dette kan føre til duplikater.

1. **Hvilke tre egenskaper er det vanligst å bruke når man ser på hvor god ytelse et nettverk har?**

De tre egenskapene som er vanlig å bruke når man betrakter nettverksytelse er:

Latency(delay), Throughput(capacity, a.k.a bandwith), og Jitter(Variability).

Latency er tiden det tar å overføre data over et nettverk fra et endepunkt til et annet.

Throughput er mengden data som kan overføres innen en gitt tidsenhet.

Jitter er endringer i forsinkelser og lengden på forsinkelsene.

1. **Hva er et DDos-angrep?**

DDos betyr “Denial of Service”. Et DDos angrep går ut på å overøse en vert med datapakker, fra en eller flere kilder, for å bruke opp alle ressurser. Dette skaper lange forsinkelser.

1. **Hva står VPN for og hva er det?**

VPN står for Virtual Private network. VPN bruker sikker kryptering for å tilby sikker aksess til et lokalt nettverk for klienter som befinner seg utenfor dette lokale nettverket. Dette er en sikker og billig løsning som bruker internett i stedet for å leie dedikerte linjer.VPN-funksjonen kan knyttes til dedikerte rutere med brannmur for økt sikkerhet.

1. **Forklar enkelt hvordan RSA-kryptering fungerer og hva en public og private key er. Det trengs ikke noen matematisk forklaring, kun en overfladisk beskrivelse på noen få setninger.**

RSA er en krypteringsmetode som benytter seg av en public key. RSA-kryptering fungerer i 3 steg: generering av nøkkeltall, kryptering og dekryptering. Hver part får en hemmelig privat nøkkel og en offentlig distribuerbar nøkkel. En melding kryptert med en offentlig nøkkel, kan bare dekrypteres med den korresponderende private nøkkelen.

Forskjellen mellom offentlig og privat nøkkel som krypteringsmetoder, er at ved privat nøkkel deler begge parter en privat nøkkel som kan brukes både ved kryptering og dekryptering. Ved offentlig nøkkel, får hver part en en privat nøkkel og en offentlig nøkkel, slik som jeg har beskrevet over.