ITGK Teori – Nettverk del 3

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

**-** TCP(transmisson Conrtol Protocol) behandler en tapt pakke ved at den bruker «positiv bekreftelse med retransmisjon». Når en pakke ankommer intakt sender mottakende software protokoll en liten bekreftelse (ACK) på suksessfullt mottak. Sender tar alt ansvar for at pakkene blir sendt. Etter at en pakke blir sendt starter en timer, og sender venter på å motta (ACK). Hvis tiden går ut sendes pakken på nytt og hvis den mottar (ACK) før tiden går ut stopper timeren.

Denne prosessen fører til at det av og til sendes kopier av samme pakke kalt ern retransmission.

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

**- Latency (delay) – Tiden det tar for å sende data gjennom et nettverk**

**-** Troughput (capacity) – Mengden data som kan sendes per enhetstid

**-** Jitter (vaiability) – Endringene i forsinkelse som oppstår og lengden på disse endringene

**c)** Hva er et DDos-angrep?

- Tjenestenekt (denial-of-service, DoS) eller distribuert tjenestenekt (distributed denial-of-service, DDoS) brukes innen Informasjons- og IT-sikkerhet for å beskrive et angrep hvor man hindrer at noen eller noe (for eksempel en person eller et system) får tilgang til informasjon eller ressurser de vil ha tilgang til.

- Kort fortalt du oversvømmer siden med pakker.

**d)** Hva står VPN for og hva er det?

- Virtual private network (VPN) eller virtuelt privat datanettverk, er betegnelsen på en datateknikk som anvendes for å skape «punkt-til-punkt»-forbindelser, såkalte «tunneler», gjennom et annet datanett (som for eksempel internett).

- En VPN-tunnel kan være kryptert, noe som er viktig når man ikke kjenner, eller er usikker på sikkerheten gjennom et eventuelt offentlig datanett, som for eksempel internett

**e)** 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 krypteringsalgoritme basert på offentlig nøkkel (en. public key).  
- Må gjennom tre steg generering av nøkkeltall, kryptering og dekryptering.  
- Meldingen gjøres om til tall M deretter krypteres det med public key n og d slik at   
N≡Md (mod n). N Sendes til mottaker som dekrypterer med privat key (e) slik at M ≡ Ne (mod n)**