Opgave 3:
b)
Det betyder at der skal etableres en forbindelse mellem serveren og klienten. Hvis forbindelsen afbrydes bliver der ikke sendt mere information. Det modsatte kunne f.eks. være en UDP broadcaster der ikke forsøger at holde en fast forbindelse men bare sender data ud i håb om at klienter selv fanger det. Det betyder også at det er vigtigt at pakkerne der sendes er intakte og korrekte. For at sikre at et TCP segment er korrekt bliver pakkens Checksum valideret ved modtagelse. Hvis ikke den stemmer bliver klienten bedt om at sende den igen. En checksum beregnes ved at lægge pakkens Header længde og Data længde sammen. Header indeholder source IP og dest IP og port.

Opgave 7:
a)
Jeg antager at med 'Authentication' menes der ift. SSL authentication. Dertil vil min forklaring være at f.eks. kan en klient og en server bekræfte hinanden vha. certifikater. Hvis man tager udgangspunkt i offentlige certifikater så ville dette gøres ved at klienten bruger et certifikat udstedt af f.eks. et Root CA service som er offentligt tilgængeligt. Ved oprettelse af forbindelsen henvender klienten sig til Root CA udbyderen og spørge om de kan validere modtagerens certifikat. Hvis alt går godt oprettes der forbindelse. Der kan også oprettes forbindelse uden brug af 3. part service. Det kræver dog at klienten og serveren har installeret de korrekte certifikater for hinanden.

Hashing defineres ved at man tager f.eks. en tekst streng og køre den gennem en matematisk funktion så der bliver lavet en ny værdi der er svær at køre tilbage til den originale værdi. Dette kan bliver gjort yderligere sværer at dekryptere vha. saltning, hvor der puttes en fast defineret værdi ind sammen med strengen så der ikke kan køre ordbogsopslag.

b)
Symmetriske nøgler kan bruges til at bekræfte en afsender fordi man ikke kan låse beskeden er sendt op uden at have den præcis sammen nøgle som afsenderen har brugt til at krypterer med. Derfor kan man sikre sig at hvis 'nøglen' ikke virker så har afsender og modtager ikke samme nøgle og der kan derfor være sandsynlighed for at pakken er blevet intercepte. Det krævede i gamle dage man fysisk udvekslede nøgler men i moderne tid bruger man for det meste det offentlige nøgle system.

c)
Jeg kan sikre mit TCP program ved at lave, eller få fat i, nogle certifikater og derefter implementere dem i systemet. Selvfølgelig skulle HTTPS også være slået til for at

denne funktionalitet kommer til at virker. Med andre ord vil jeg lave en secure socket forbindelse mellem klient og server frem for en almindelig TCP socket forbindelse, som jeg gør nu.