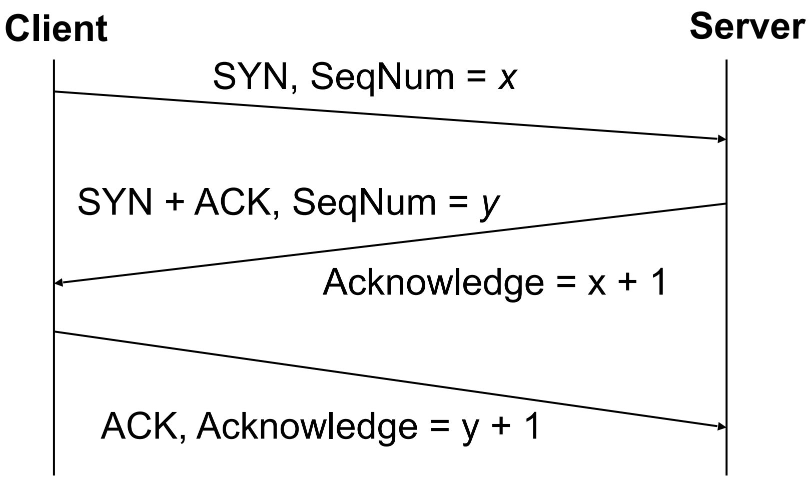
4.

a) UDP adds only simple multi-plexing to the underlying IP network, to allow more than one stream of data to travel between a pair of hosts [1]. Data must be placed by the application into packets [1] and there is no guarantee of delivery, packet order or non-duplication. [1]
TCP adds considerably more functionality. It requires an explicit setup and disconnection [1] and unlike UDP provides a byte stream interface [1] in which the application can write data arbitrarily and the protocol layer will packetise it and reassemble it. Delivery in TCP is guaranteed [1], as is packet ordering [1] and an additional checksum ensures correct data [1]. TCP is also a full duplex connection [1] providing data flow in both directions and implements flow control [1] in both directions.

b) Ports are used in both UDP and TCP to allow multiplex connections between the same pair of hosts [1], i.e. more than one data stream at the same time [1]. Ports also provide the means by which data streams are associated with particular applications [1]. An application "registers" itself with a particular port number and all data received on that port will be passed to that application [1]. Some common applications always have the same port number and thus allow standard connections to be made, for example a web server is usually found on port 80. [1]

c) [diagram below or equivalent narrative description] [6]



If the original SYN is lost the no acknowledgement will be received and the client will simply retransmit. If it is duplicated the duplicate packet can be identified by its sequence number and discarded. [2] If the SYN+ACK is lost then the client will timeout and can attempt a new connection start with a new sequence number. If duplicated, the acknowledge sequence number can be used to detect this. [2] If the ACK is lost this may cause a problem and is the vulnerability exploited by some denial of service attacks. Duplication of the ACK is again detected by the sequence number [2].

d) Compression is not free as it takes computing time and resources to undertake the compression and expansion [1]. Some data is not appropriate for compression, for example small amounts of data, or data that contains a very high level of randomness [2]. Over a transmission network there is no benefit if the total transmission time is not decreased [1], i.e. the time taken to compress and decompress the data and transmit the compressed data must be less than the time taken to transmit the raw data. [1] This will depend both on the compression and decompression time and on the compression ratio available [1]

5.

a) The public and private keys are mathematically related such that data encrypted with the public key can be decrypted with the private key. [2] It is important that although there is a mathematical relation between the two keys that it is very difficult to determine the private key given the public key. [1] The public key can be made known generally, the private key must remain secure [1].

bi) Authentication is the means by which a person or program proves their identity [2], for example by use of a password. In a secure network it ensures that only authorised users or programs have access to resources [1].

bii) Message integrity is proving that a message that has been received is identical to the message as sent, for example by using an MD5 checksum [2]. In a secure network it is used to ensure that messages have not been altered during transmission [1].

biii) Non-repudiation means that a person or program cannot later deny that they sent a message, for example by placing suitably encrypted copies of messages with an escrow agent [2]. This is used in a secure network to ensure that actions cannot be denied.

c) Images to be JPEG compressed are first broken down into chrominance and luminance [1] and then into small square areas, which are transformed into the frequency domain using the discrete cosine transform [1]. This results in a matrix of frequency coefficients across in that small area. [1] These coefficients are then quantized, i.e. certain of the higher frequency coefficients are discarded. [1]. The quantisation tables that are used can be varied to suit the requirements of the user, for maximum compression the tables contain many zero values, discarded many frequencies, for maximum quality almost all frequencies are retained [3].

di) SMTP is used to transmit an e-mail from a mail client to a mail relay host for onward transmission to the recipients server [2].

dii) MIME is used to encode attachments to e-mail by adding a header to the e-mail with details of the contents [2].

diii) POP3 is used by an e-mail client program to retrieve incoming messages from their mail server [2].

e) If the sender attaches a JPEG image to an e-mail then this will be encoded using MIME [1]. Additional MIME headers will be added to the e-mail stating that there is an attachment, listing its type [1], which encoding has been used [1] and what the separator line is between the body of the e-mail and the encoded attachment [1]. The e-mail program will then use SMTP to send the e-mail with the attachment to the local server [1] which will then forward the mail to the recipients mail server. The recipient e-mail client will use POP3 to download the e-mail [1] and examine the header to determine the type, location and encoding of the attachment [1].