2017 Network and Communication Examination Solution

1. a. `nslookup -type=MX diktion.net` and `telnet smtp.diktion.net 25`

   b. **1** The IP of the server might be blocked by the firewall on the router/local computer. **2** Web server might be under maintainence.

   c. The utilization of the line would be

   $$\frac{\frac{16 \times 10^6 \cdot 8}{32}}{24 \times 10^6} = \frac{1}{6} \approx 16.67\%$$

   The utilization could not reach to 100% because **1** the round trip time must be 0 in ordeer to achieve 100%, which is not possible. **2** Someone else is jamming the connection, such as another user downloading a large file in the same LAN or lots of poeple are downloading the same pdf at the same time. **3** The server side only supports connection up to $\frac{16 \times 10^6 \cdot 8}{32} = 4\ \text{Mbps}$.

   d. Public free and open network is vulnerable to attacks and monitoring. Anyone can sniff packets through software such as Wireshark, especially when some protocols send plain text rather than encrypted text, such as SMTP. If the email/packets contain confidential information, they are subject to be stolen/exposed to the attacker. Or even worse: the attacker can start another WiFi with the same SSID so that the attacker can see all the traffic on the workphone. (Man-in-the-middle attack)

   e. TCP. Though the service is paid, the streaming service still needs stability over speed. Additionally, the software will buffer part of the video so that it will be loaded faster. Since all the content will be pre-recorded, there is no need to use UDP as it does not need to be rendered in almost real-time.

   f. The public key of Alice is $9^2 \bmod 11 = 4$ and the public key of Bob is $9^5 \bmod 11 = 1$.

   Then we can calculate their shared secret key: $4^5 \bmod 11 = 1^2 \bmod 11 = 1$

   The encrypted text is thus shifted to the right on the alphabet table by 1: `IFMMP`

2. a. i) BGP is responsible for controling inter-AS routing that include reachability information from neighbour AS and determine goodroutes to destinations in other subnets. It belongs to the Network Layer.

   ii) Shannon's Law states the theoretical limit of data transmission/communication. It relates to the Physical Layer

   iii) Token passing refers to the way of frame transmission between different hosts connected together using ring topology. It belongs to the Data Link Layer.

   iv) Ethernet switch is a device used to connect many devices to the same network and work as a wired repeater to send frames to the correct host. It belongs to the Data Link Layer.

b. i) Field A => Total Length

Field B => Time To Live

Field C => Source Address

Field D => Destination Address

ii) The `vers.` field indicates which IP version is being used in this header(IPv4 or IPv6). `hlen` indicates the length of this header in bytes, which should be 20. `type of service` is used for different purposes, particularly in prioritizing IP datagram. `identifier` is used as an id for the IP datagram so that it does not repeat within certain length/lifetime. `flag` indicates whether there are more fragments follow this one. `fragmentation offset` indicates the offset of the original datagram(e.g. UDP datagram of size 65535 bytes) during fragmentation. `protocol` indicates the protocol being used in this datagram transmission, such as TCP, UDP, etc. `header checksum` is the computed checksum value of this header.

iii) `flags`, `fragmentation offset` can be discarded because IPv6 pushes end calculation into the end system rather than the network.

`hlen` can be replaced because the header length is fixed (40 bytes)

`type of service` is replaced by the `traffic class` field (thus it is NOT entirely disgarded)

`identification` and `checksum` can be discarded as well since IPv6 datagram rarely corrupts or could be handled by higher protocols.

iv) **1** There are not enough bytes to store the source and destination address in the Ethernet frame. **2** The current network infrastructures (software) might need significant changes in order to adapt this. **3** It's harder to add new rules/protocols on top of Ethernet frame: we do not want to change Ethernet frame format in order to achieve something that is related to the Network Layer, such as hop count. (make things more complicated) **4** The data fragmentation now needs to be handled directly by the transport layer as the Ethernet frame has a maximum limit of 1500 bytes (including Ethernet II header).