1. Provide 200-300 word summary of the article on "Reflections on Trusting Trust" by Ken Thompson
2. Provide 200-300 word summary of how Internet (including it's security) was designed by watching Youtube talk by David D. Clark

Answer:
Reflections on Trusting Trust:
The article is about to what extent that one can trust whether the program is free of bugs and “Trojan Horses”. The answer to that is you cannot trust the code unless it is written by you. But it is not practical to write the code for all the software that we use. So we instead search for any bugs or trojan horses in the source code written by other programmers. We can able to find some bugs and can able to fix them. But as the level of the program gets lower and lower it would be much harder to detect these bugs or trojan horses. Even some of these bugs might be due to some mistake or kept intentionally. The misbehavior of being attacked on the web today is not due to implementation bugs but due to deliberate design decisions. Inspecting code to see whether it’s trustworthy or malicious is a fool’s errand. The only way that we can reliably have downloads of active codes is that you have a very clear sense of whether the sender is trustworthy.

Designing of the Internet and its security:
The Internet started in the 1970s where initially it is just trying to get the protocols to work. In the 1980s it was involved in making the hierarchy(routing, exterior gateway protocol, interior gateway protocol, DNS hierarchy, organizing the standards committee) to scale it big. Until the 1980s the core of the internet was NFSNET run by NFS. But In the 1990s it started to get commercial in which the BGP(border gateway protocol) has played a major role in shaping industry structure.

In the first part of the 1990s concerning the quality of service DiffServ and IntServ were designed by the NSF but the ISP rejected to deploy them in their networks as it will cost them a lot but they are not able to make a profit out of it instead it will provide a high economical growth to apps running on top of the IP layer.

When concerning the security of the internet, it is a multi-dimensional space in which different objectives compete with each other and different stakeholders compete with each other. So building a successfully secure internet is to build a compromise in which all these actors will allow your solution to survive.
These security problems can be classified into four types:
Third-party trying to interfere(steal, modify, block) in the communication between two trusted people
I connect to you and you attack me - malicious attachment downloads.
Mechanisms of the internet - broken by themselves.
Denial of Service attacks
Even after knowing the existence of vulnerabilities, the reason why it couldn’t able to fix them is due to the people not able to agree on what the problem exactly is and the people who suffer from are not the people who would have to pay(negative externality). The three elements of information security include confidentiality, integrity, and availability(CIA triad). The main problem of encrypting everything doesn’t solve availability.

Even though the internet move packets pretty well, the reason for proposing alternatives is to do something different not to do what exactly it does but better than what it does.