1.

(a) Mistake: Bob uses a 128-bit public key in RSA.

He should generate 2048-bit or 4096-bit public/private key by RSA because 128-bit key is too short to securily encrypt message.

(b) Mistake: Bob asks the CA to sign his private key

He should ask the CA to sign his public instead of private key, because if the CA signs his private, everyone will have the private and all message sent by Bob will be decrypted.

(c) Mistake: Bob asks Alice to do the salt and hash.

He should do the salt and hash for Alice’s password and store the results. Because the user may not know cryptography. This breaks the rule of psychological acceptibility.

(d) Mistake: Bob encrypts Alice’s password and store it.

He should hash the password and store the hash value so that if the hacker attack his database, he can not directly know the password. Otherwise, once the attack can decrypt the password, they can directly steal the account.

2.

(a) IP Spoofing: Ingress/egress filtering. Ingress filtering can prevent outside attacker spoofing the adress of an internal machine. Egress filtering can prevent attack using internal machines to perform attack.

(b) Eavesdropping: Proxies. MITM can not know the source IP and destination IP at the same time. The user can hide their IP and the destination IP by using proxies.

(c) Teardrop Attack: Deep Packet Inspection. Because DPI can look into the packets to see if two packets contracting each other. If two packets contract each other or they are possible to perform Teardrop attack, the DPI will block them.

3.

(a) Guard flag only relays have more amount of advertise bandwidth than exit flag only relays.

Explanation: The relays that has more bandwidth and performs better in speed are selected as guard flag relays by the Directory Authority.

(b) Downloading rate is much higher for a 50 MiB file to the op-hk onion server than a 50 KiB file. The files of small size do not make use of small portion of total bandwidth and files of larger size make use of larger portion of total bandwidth. Therefore, downloading rate for larger files is higher because of more bandwidth.

(c) Disadvantage: The browsing speed is lower, and latency is higher because data will be transmitted through three relays.

Advantage: Anonymity. The MITM can not know the user IP and destination IP at the same time so that the behavior of the user is secret.

(d) Turkey: the ratio is around 0.8

The reason may be that the Turkish government block some websites like and the Tor service. Therefore, most of Turkish people need to use Tor bridge to connect to Tor net and visit the banned websites.

Programming assignment part (b)

(a) The responding time of the websites is much longer, and the latency is higher when using Tor browser than normal browser because of packets need to go through 3 relays from website to browser.

(b) Visits are blocked from some websites. For example, google search is not available, and a returned result shows google detects the unusual traffic from the user’s computer network. Sometimes, the connection will be interrupted by errors like error 400 because some relays are not stable enough.

(c) The location service shows different results. When visiting youtube.com in Hong Kong using normal browser, usually the page will directly show Youtube hk and the contents are related to Hong Kong. However, if the visit is through Tor net, the page will instead show, for example, Youtube fr or Youtube jp, which will be the location of the exit relay in the corresponding Tor circuit.

(d) No history is stored in the browser. After visiting some websites, the history will not be shown in the history session of Tor browser.