CSCI368 NETWORK SECURITY ASSIGMENT 2 SUBMISSION

TIMOTHY MAH

8750634

[txamah001@mymail.sim.edu.sg](mailto:txamah001@mymail.sim.edu.sg)

1. where should K be derived from?

ans:

the K shared secret key should be derived from A secret key and B public key

2. This protocol uses key transport or key exchange?

ans:

this protocol uses key transport exchange because the shared secret key is not sent to each other

3. Alice said sending certificate and pk is useless in this protocol. Justify what Alice has said

ans:

sending a certificate is useless because A is already sending Sig(sk, M), which acts as a signature. and sending A's public key is useless because A has already sent A's public key in g^b

4. What is the most significant security issue if the signed M includes g^a, g^b only without the Message from B?

ans:

an attacker could spoof this signature because g^a and g^b are public keys that can be intercepted with man in the middle attacks

5. What is the potential security issue if CA forgets to include “subject” in the signed message when generating certificate for A?

ans:

the certificate may be invalid because subject could contain information to identify A is authentic hence the certificate could be spoofed by an attacker

6. If A and B run the UDP protocol to complete the communication, what could happen at the end of this protocol?

ans:

the message is not confirmed to be received as a whole or even accurately because UDP does not perform integrity check