CS5285: Information Security for eCommerce Autumn, 2024
Tutorial 6, Week 8 (October 25)

Question 1

What is the main issue with the following protocol and how would we fix it? Would the issue still be there if message 2 was Sig_A(N)?

1: A < B: RB
2: A > B: E_K(RB)

Question 2

Could N be any type of nonce in this protocol?

1: A < B: E_K(N,A)
2: A > B: N

Question 3

Design a unilateral authentication protocols using

a) A timestamp and an encryption mechanism

b) A timestamp and a MAC mechanism

c) What is the practical difference in how we send the timestamp between a) and b)?

Question 4

You are asked to design an authentication protocol whereby a web client can authenticate servers he wishes to visit. You must make the following decisions and design the most practical protocol....

- Time stamp or nonce?

- Symmetric or asymmetric mechanism?

To make your decision think about: How many clients and servers? What can we assume about clients?

Question 5

You are asked to design an authentication protocol whereby a client can log onto online banking.

You are asked to do so for two banks - both banks gives the client a secure hardware device that can generate a response.

a) Bank 1 device has a single button, and response is generated upon press of button.

b) Bank 2 has a small 10-digit numeric keypad, and also a button to press for response generation?