COMP90007 Internet Technologies

Week 12 Workshop

Semester 2, 2019

Question 1

Given the RSA algorithm we studied last week, if p = 3, q = 11 and if d = 3 and e = 7 instead of the version we saw in class, using the same character mapping we saw in class though, where A is 01 and B is 02, and C is 03 and so on, how would RSA work? Would it work at all? Show in detail what numbers would be computed and transmitted at both ends of a transmission if we want to send across a "D". Show where it fails if it does not work properly?

Question 2

Using the RSA algorithm we saw in class, please design a simple algorithm to sign documents where the sender cannot refute the fact that a document was signed by herself later on. Which property of RSA your algorithm relies on?

Question 3

Given the Diffie-Hellman key challenge in the lectures, please develop the full flow chart for the man-in-the-middle (MITM) attack, with step numbers and messages sent, show details about how this attack would work.

Question 4

Leveraging the authentication protocol using Public-Key cryptography, we send across two additional numbers, RA and RB. Why are these needed? Why not Alice sends only her name to Bob but needs a RA as well?

Question 5

Please list, summarize the four key areas/aspects of network security.