CS 558 Introduction to Computer Security, Spring 2024
Written Homework Assignment 2
Total points 100

Out: 2024 Apr 28
Due: 2024 May 4 Sat. 23:59:59

Unnecessary long answers are usually from generative AI. Refer to the submission instructions for details of penalties.

1. (15 points) In our class, we demonstrated that mutual authentication can be established using symmetric keys as illustrated in the Figure 1. Now, modify this protocol to incorporate a hash function in place of symmetric key encryption to ensure the protocol remains secure.

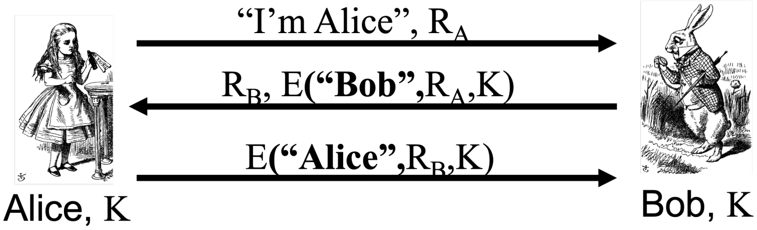

Figure 1: Mutual Authentication with Symmetric Key

2. (30 points) Based on protocol in Figure 1:
(a): Make modification to the protocol to establish a session key.
(b): Based on (a), design a protocol use two messages.

3. (25 points) Consider the simplified SSH protocol in Figure 2 we have discussed in the class. One variant of the protocol allows us to replace Alice's certificate, certificate$_A$, with Alice's password, password$_A$. Then we must also remove S$_A$ from the final message. This modification yields a version of SSH where Alice is authenticated based on a password.
(a): What does Bob need to know so that he can authenticate Alice?
(b): What are the significant advantages and disadvantages of this version of SSH, as compared to the version in Figure 2 which is based on certificates?

4. (15 points) Consider the SSL protocol in Figure 3 that we have discussed in the class.
S is known as pre-master secret, randomly generated.
K = h(S, R$_A$, R$_B$.)
"msgs" means all previous messages.
CLNT and SRVR are constants string.

Modify this protocol so that the authentication is based on a digital signature. Your protocol must provide secure authentication of the server Bob, and a secure session key.

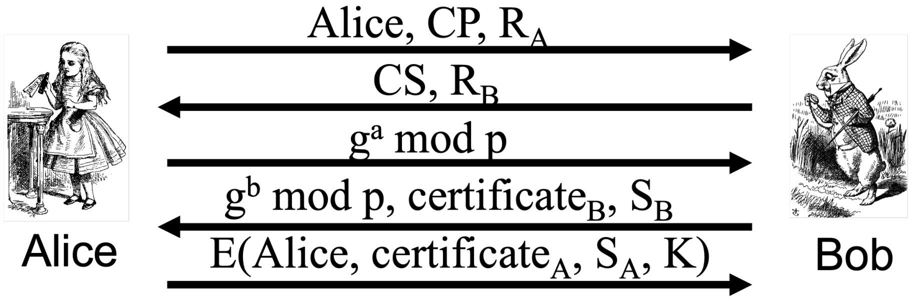
Alice, CP, R_A
CS, R_B
g^a mod p
g^b mod p, certificate$_B$, S_B
E(Alice, certificate$_A$, S_A, K)
Alice
Bob

Figure 2: Simplified SSH

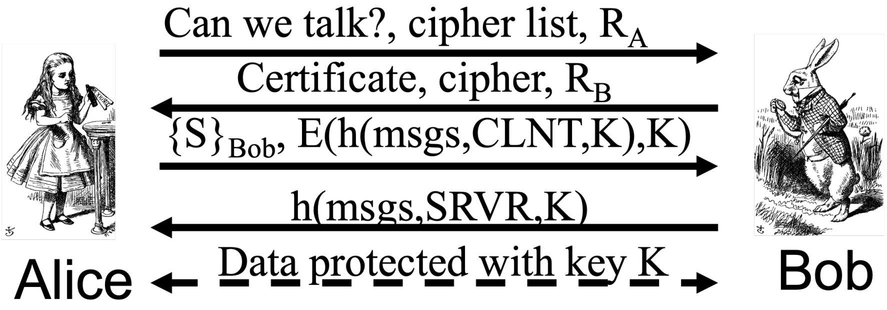
Can we talk?, cipher list, R_A
Certificate, cipher, R_B
$\{S\}_{Bob}$, E(h(msgs,CLNT,K),K)
h(msgs,SRVR,K)
Data protected with key K
Alice
Bob

Figure 3: Caption

5. (15 points) IKE has two phases, Phase 1 and Phase 2. In IKE Phase 1, there are four key options and, for each of these, there is a main mode and an aggressive mode.
a. Explain the difference between Phase 1 and Phase 2.
b. What is the primary advantage of Phase 1 public key encryption main mode over Phase 1 symmetric key encryption main mode?

Submission instructions

- Type your answers using whatever text editor you like, remember to include the index number of each question.
- Export the file to PDF format.
- Name the PDF file based on your BU email ID. For example, if your BU email is "abc@binghamton.edu", then the PDF file should be named as "hw3_abc.pdf".
- Submit the PDF file to Brightspace before the deadline.
- Do not copy/paste answers from generative AI(ChatGPT like tools). Once detected, you will get 0 out of 100 points. Long answers are often flagged as potentially copied from generative AI tools and will be checked for originality.
- Do not copy other students work. Once detected, this behavior will be tread as plagiarism.