CS458-01/02/03 - Fall 2018
Practice Problem Set 1
No submission is needed

Problem 1

Describe Diffie-Hellman key exchange in modular arithmetic, and list public and secret parameters. How are the personal public parameters calculated from the secret and the general parameters? How is the shared key calculated?

Problem 2

In the Diffie-Hellman key-exchange algorithm between `Alice` and `Bob`, an intruder `Eve` is able to break the security of algorithm only if `Eve` can find the secret key of `Alice` and the secret key of `B`. Do you agree? Justify your answer.

Problem 3

What is the technical difference between a Message Authentication Code and a digital signature? What are the effects of this, in terms of who can create a MAC, and who can create a signature? Who can verify a MAC, and who can verify a signature?

Problem 4

Which protocol would you use to send an encrypted email to your friend, DH or RSA? Justify your answer.

Problem 5

What hard problem does Diffie-Hellman protocol depend on? What hard problem does RSA depend on?

Problem 6

Bob received a 128-bit AES key and the message "from Alice: use this key to send me your credit card number", both encrypted with his public key. Should he do what the message says? Assume Bob does want to send Alice his credit card number.

Problem 7

We discussed "meet-in-the-middle" attack. We also talked about "man-in-the-middle" attack. They are completely different concepts, despite their similar names. Explain what each attack is.

Problem 8

It is common practice to salt the user's password in addition to hashing. What attack does this practice prevent?

Problem 9

What is the purpose of including Message Authentication Code (MAC) with the message? What is the difference between a MAC and a HMAC?

Problem 10

Who generates the authenticator in Kerberos and what is the purpose of the authenticator?

Problem 11

Does using passwords with salts make attacking a single account more difficult than using passwords without salts? Explain why or why not

Problem 12

Suppose Alice wants to send a message to Bob containing her name `N`, her computers IP address `IP`, and a request `R` for Bob. Design encrypted messages that Alice must send to meet the security requirements below. Suppose that $K_{pr,A}$ and $K_{pr,B}$ are the private keys of Alice and Bob respectively. Assume that Alice and Bob share a symmetric key `K` and have securely distributed their public keys $K_{pub,A}$ and $K_{pub,B}$ to each other. Assume that all the messages include Alice's name, IP address, and the request.
Recall the notation that `x||y` means the concatenation of `x` with `y`, $e_k(x)$ denotes the encryption of `x` using key `k`, and that `h(x)` denotes a hash of `x`. Using the notation above, answer each question below. Be specific about what is computed, what is transmitted, and who the sender and receiver of the message is.

i. Using the symmetric key, design a message that enables Bob to verify that the messages integrity has not been violated and that it is from Alice.

ii. Using the symmetric key, design a message that protects the confidentiality of the request and ensures that Bob can verify the messages integrity and source.

iii. Using public key cryptography, design a message that enables Bob to verify that the messages integrity has not been violated and that it is from Alice.

iv. Using public key cryptography, design a message that protects the confidentiality of the request and ensures that Bob can verify the messages integrity and source.