ECE424: Network security

Homework 4
Due: 11/20/2024

Collaboration Policy. Each student must hand in their own answers. Use of partial or entire solutions obtained from others or online is strictly prohibited. However, discussing the problems with other fellow students or forming study groups is encouraged.

Submission Format. Please submit your solutions electronically through Canvas as a **single PDF file**. This file should include both your code and clear explanations of each step involved. Ensure to also provide the **outputs** generated by your codes.

Provision of Prime Number and Primitive Root. Please use the provided prime numbers and the corresponding primitive roots to solve the questions.

Q1. *Secure key exchange over a public channel.* Alice and Bob would like to communicate over a public channel. They want to establish a shared secret key to secure their communication.

(a) Implement the Diffie-Hellman algorithm with the provided prime number and primitive root. A shared key will be established secretly. Run your code and check if Alice and Bob generate the same key. The outputs should include

1) (**5 pts**) Alice's secret integer x and the message A to Bob,
2) (**5 pts**) Bob's secret integer y and the message B to Alice,
3) (**5 pts**) The key generated by Alice,
4) (**5 pts**) The key generated by Bob,
5) (**5 pts**) A verification that Alice and Bob generate the same key.

Prime number (**p**): 102188617217178804476387977160129334431745945009730065
519337094992129677228373.

Primitive root ($\boldsymbol{\alpha}$): 2.

(b) The Diffie-Hellman algorithm is a method for key exchange, in which Alice and Bob collaborate to find a shared key. Next, we want to explore the case where Bob generate a secret key and shares it with Alice using RSA algorithm. Generate a random number as key and implement the RSA algorithm. Check whether Alice recovers the key generated by Bob. The outputs should include

1) (**5 pts**) The key k generated by Bob,
2) (**5 pts**) The public key k_e and private key k_d generated by Alice using RSA,
3) (**5 pts**) Encrypt the key k (generated by Bob) to generate ciphertext c using the public key k_e,
4) (**5 pts**) Decrypt ciphertext c using the private key k_d,

5) (**5 pts**) A verification that Alice recovers the key generated by Bob.

Prime number (**p**): 61.

Prime number (**q**): 53.

Q2. *Digital signature authentication.* Alice and Bob would like to authenticate the identity of each other.

(a) Implement the ElGamal authentication method with the provided prime number and primitive root. The outputs should include

1) (**40 pts**) A documentation of all procedures and intermediate results,

2) (**5 pts**) A successful authentication when the message is unchanged,

3) (**5 pts**) A failed authentication when the message is altered.

Prime number (**p**): 1021886172171788044763879771601293344317459450097300655193370949921296772283 73.

Primitive root ($\boldsymbol{\alpha}$): 2.

Q3. (**10 pts**) (**Optional**): Although malicious user may not decrypt the ciphertext between Alice and Bob, she/he can replay the previous ciphertext to fool/jam the system. Implement a feature to timestamp the communication. Show sufficient explanations and outputs to demonstrate the effectiveness.