INFO 102 Lab 11: Secret communication

Partner #1: Name: _____ Net ID: _____

Partner #2: Name: _____ Net ID: _____

Define the following terms related to secure communication Partner 1: Authentication Partner 2: Confidentiality Partner 1: Integrity
Define the following terms related to access control Partner 2: Authentication Partner 1: Authorization Partner 1: The principle of least privilege
Why is it less secure to install a browser extension that changes how the window border looks than it is to visit a webpage that is running complicated code that you don't understand or trust?
What are the two most important tips for using computers safely? 1. 2.

On the course labs page, use the “Simplified cryptography tools” and the Lab 11 channel for your section in course Teams account.

Compose two truths and a lie. All three will be shared in the steps below.

Truth 1:

Truth 2:

Lie:

Share a message in teams channel containing

1. Your public key
2. In a random order,
    a. Truth 1 and its signature
    b. Lie and its signature

Pick another team in your lab and check their message’s signatures. Reply to their message with a comment about their true message.

Pick another team to communicate with in secret. What team did you pick?

1. One team post a random value on the team, tagging the other team using an @ in the message.
2. Both teams,
    a. Pick another random value you don’t post
    b. Use the key exchange function to combine the value from steps 1 and 2.a; share that as a reply to the random value post
    c. Use the key exchange function to combine the value the other team shared in step 2.b with the one you created in 2.a; don’t share this, it’s your secret symmetric key cipher
    d. Encrypt your other truth with the secret symmetric key cipher and post the encrypted result as a reply to this thread
    e. Decrypt the other team’s post. What was their message? Write it here

When you’re done, check out with a TA or CA and hand over this completed worksheet.

Bye!