CSCI 4331/6331 November 11, 2024

Quiz 7

Name:

In this quiz, you are asked to show how to turn the Diffie-Hellman (DH) key exchange protocol into a public-key encryption scheme. The following questions are meant to guide your construction:

1. Recall that as a result of DH key exchange, Alice and Bob both output a random-looking group element g^{xy}. Assuming that the message $m \in \mathbb{G}$, how can you use this shared key to "encrypt" m?

2. The DH key exchange protocol is interactive, while we want a public-key encryption scheme to be non-interactive. How can Alice use the first message of DH key exchange to produce a public key?

3. Describe how Bob can use this public-key to encrypt a message to Alice. (Hint: Remember that encryption must be randomized).

4. Describe the corresponding decryption procedure.