In-class exercise -- Crypto
CS 642 -- Spring 2016

Alice wants to send a long, encrypted message to Bob over the internet. Assume both Alice and Bob have each other's public keys. Give the steps for Alice to prepare the message to be sent.

Bob receives Alice's message. He keeps his private key stored encrypted under a passphrase. Draw a diagram or give a formula for the password-based key derivation function.

Give the steps for Bob to recover and validate the message he received from Alice staring with his password, encrypted public key, and encrypted message from Alice as inputs.