Q1: Using the cryptographic building blocks that you’ve already learned about, give the steps involved when Alice sends a (long) encrypted message to Bob. Consider only encrypting the message with Bob’s public key (you don’t need to sign it with Alice’s private key).

Also give Bob’s steps for decrypting the message. Bob’s private key is stored encrypted, under his passphrase, on his computer.
Q2: Using the cryptographic building blocks that you’ve already learned about, give the steps involved for Alice and Bob to establish a “secure channel” (like TLS/SSL and SSH). After negotiating the secure channel, Alice and Bob should both share (typically multiple) symmetric keys.

Let’s talk securely; here are the algorithms I understand

I choose these algorithms; start key exchange

Continue key exchange

Communicate using exchanged key