







10. Alice and Bob wish to share a symmetric key. One way to do this is for them to run Diffie Hellman. Another way, if they already have each others' public RSA keys, is simply for them to use public key encryption to exchange a key. Compare and contrast these two approaches. Which one is more secure? Is there a way to make the RSA scheme more secure than the naive approach of just having Alice encrypt a random key with Bob's public key and sign it? If so, give a protocol for that. (8 points)