Alice and Bob are playing an online dice game where they must roll virtual dice representing the 6 sides of a physical dice. However, they do not trust each other and suspect that, if they can just roll dice locally on their computers, they will choose the outcome of the dice dishonestly, choosing the outcomes they need in order to win the game. In order to solve this, they want to execute a protocol among themselves to roll a dice while ensuring that they obtain an honest dice rolling outcome. Unfortunately, Alice and Bob are also using an insecure network, where they have no authenticity, confidentiality and integrity guarantees.

How can Alice and Bob play an online dice game over their insecure network when they do not trust each other?

Luckily Alice and Bob are security savvy and just had lectures on advanced cryptography and secure channels. Moreover, they have access to a Public Key Infrastructure, meaning that they know each other's public keys for a digital signature scheme.

Your assignment is to do the following steps help Alice and Bob:

1. Design a protocol that allows Alice an Bob to throw a virtual 6 sided dice over the insecure network even though they do not trust each other.

2. Explain why your protocol is secure using concepts from the lectures.

3. Implement your virtual dice protocol in a programming language of your choosing. The implementation must consist of a program representing Alice and another program representing Bob that communicate over a network (two processes running on localhost is ok). You can use any libraries or programming languages of your choosing.

You must hand in a report explaining your protocol and why it is secure as well as the code implementing your protocol.

You can choose the digital signature scheme used by Alice and Bob, meaning you can choose how their public and secret keys for the digital signature scheme looks like.

HINT: Rolling dice is just sampling a random number from 1 to 6.