

## 3.3 Question 3

**3.3.A** In the Diffie-Hellman protocol, each participant selects a secret number  $x$  and sends the other participant  $g^x \bmod p$  for some public number  $g$ . What would happen if the participants sent each other  $x^g$  for some public number  $g$  instead? Give at least one method Alice and Bob could use to agree on a key. Can Eve break your system without finding the secret numbers? Can Eve find the secret number

As  $g$  is a publicly known generator, Eve can easily compute the secret number  $x$  as the "Indiscrete Logarithm Problem" is not hard - therefore the security is not given anymore.