3.3 Question 3

3.3.A In the Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant $g^x\ mod\ p$ for some public number g.

What would happen if the participants sent each other $x^g\ mod\ p$ instead

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.

Suggest a method that the participants could apply for generating a common key (using the $x^g\ mod\ p$ approach)

Both Bob and Alice exchange $x^g\ mod\ p$ and $y^g\ mod\ p$ and then both can compute $x^g * y^g\ mod\ p$, which will be the same as $(xy)^g\ mod\ p$.

Can Eve break your system without finding the secret numbers?

Yes, Eve can use the eavesdropped information she got and multiply both of those modulo p and gets the same solution as Alice and Bob are receiving by following the mentioned protocol.

Can Eve find the secret number?

Yes, as finding the secret numbers of Alice and Bob is known as the "Indiscrete Logarithm Problem" which is not hard.