16-124-836
Marcel Matti ZAUDER

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 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.
For example Alice and Bob can agree on the public number $g = 4$. Then each of them chooses a secret number - i.e. Alice chooses 5 and Bob 7 - and then computes x^g - which is $5^4 = 625$ and $7^4 = 2401$, respectively. Both Alice and Bob exchange these numbers via a public medium which Eve can eavesdrop. As previously mentioned the "Indiscrete Logarithm Problem" is not hard and with the knowledge of the public number Eve can compute both secrets.