Question 3:

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

  - What would happen if the participants sent each other $\boldsymbol{x^g}$ **mod** $\boldsymbol{p}$ instead?
  - Suggest a method that the participants could apply for generating a common key (using the $\boldsymbol{x^g}$ **mod** $\boldsymbol{p}$ approach).
  - Can Eve break your system without finding the secret numbers?
  - Can Eve find the secret number?