Two experiments about the Diffie-Hellman protocol – COSC-3325-01

1. In order to simulate the Diffie-Hellman protocol, let us consider three teams of students, one team called Alice, another team Bob, and another team Eve. The Alice team and Bob team want to securely communicate. Note that the Eve team is an eavesdropper because it has access to all communications between Alice and Bob teams. All teams are equipped with a calculator, paper and pencils, as well as the Diffie-Hellman protocol description.
The purpose of this exercise is to use the Diffie-Hellman protocol for:

a. Establishing first a secret shared key between Alice and Bob teams.
b. Using this key, Alice and Bob teams have to communicate one another, say with a symmetric cryptographic algorithm (like Caesar algorithm).
c. The Eve team should try their best to identify both the key and the later messages transmitted.

2. After this experiment, try to identify what measures the Diffie-Hellman protocol should have implemented in order to make it resistant to such attacks. The Caesar symmetric cryptographic algorithm is replaced by a "random" generation permutation of the alphabet known only to Alice and Bob. In fact, these two teams have an entire list of such permutations. The secret shared key is obtained in the same way as described in Exercise 1, but that key should be used to identify which secret permutation (that is, unknown to Eve) is used by both Alice and Bob for their later communication. Again, the Eve team should try their best to identify both the key and the later messages transmitted.

3. After the two experiments, answer the following questions:

a. Were these two experiments useful? Why?
b. Were these experiments ethical?
c. Why do we have to pretend be bad guys when we data have to be transmitted in networks?
d. How easy was for Eve team to break the key and the later messages, if applicable?
e. Were the Alice and Bob teams concerned about the security of data transmission, such as the fact that the key is not strong enough or the Eve team might have good luck and simply guess the key?