Crypto exercise

1. **Ceasar cipher**
   a. I will split the class in teams of three.
   b. One person A (Alice) will encrypt a message that I give you in a piece of paper using the Ceasar cipher.
   c. The second person B (Bob) will decrypt.
   d. The encrypted message will be passed in the clear so that the third student E (for Eve the Eavesdropper!) will see the message.
   e. We will run two scenarios:
      i. The two people that communicate exchange the key that they used in secret successfully, therefore Eve has to try to figure out the key to decrypt the message. In this scenario, Eve will first use his/her brain, then the tool: [http://md5decrypt.net/en/Caesar/](http://md5decrypt.net/en/Caesar/) to decrypt.
      ii. The two people share unsuccessfully their key and Eve can intercept it.

2. **Answer the following questions:**
   a. What was the methodology that Eve used to break the cipher when she had and did not have the key?
   b. What was faster and why?
   c. How can you solve the problem of Eve intercepting the key?

3. **RSA public key cryptography**
   a. I will give you public/private key pairs, one per team. All team members will know the public key, even Eve. Only Alice and Bob will know their private key.
   b. Alice will send to Bob a random number, Bob will try to decrypt it with his private key, and Eve will intercept and try to break this with any online tool she wants.

4. **Answer the following questions:**
   a. Was Eve successful and why?
   b. How can we make Eve’s work even more difficult?