

Review Questions 17

Your Name:

Please print out this form (two-sided, if you can) and write your answers *legibly* in the spaces provided. If you can't write legibly, type.

1. Explain the difference between confidentiality and integrity of messages. Can you have one without the other?

2. In the block cipher shown in Figure 8.5, how many bits are needed to represent a key?

3. Suppose we want to construct an RSA key pair based on the initial values $p=5$, $q=11$. Is 15 an acceptable value for e ? Is 27? (Ignore the fact that these values are all too small.)