

Homework 7

Due at the *beginning* of class on Dec. 7

You may use a calculator for these problems, if needed. (I recommend the command-line utility `bc` on a unix system, which handles “large” numbers and modular arithmetic.)

1. Consider an execution of Diffie-Hellman key exchange in the group $\mathbb{Z}_{17}^*$ with generator 3, where Alice chooses exponent $x = 9$ and Bob chooses exponent $y = 3$.
 - (a) What is the message that Alice sends Bob?
 - (b) What is the message that Bob sends Alice?
 - (c) Compute the key that Alice and Bob each derive, and verify that they are equal.
2. This question concerns padded RSA (as in Construction 10.18). Say $N = 55$, $e = 3$, and $d = 27$. Note $||N|| = 6$, as N in binary is 110111.
 - (a) Say $\ell = 3$ and we encrypt the message 010 using random bits 11. What is the resulting ciphertext?
 - (b) Show the steps of decryption, and verify that the original message is recovered.
3. Exercise 10.1.
4. Exercise 10.11.
5. Exercise 10.17.
6. Exercise 12.2.
7. Exercise 12.4.
8. Exercise 12.7.