ECE 371: Introduction to Security Engineering

Homework 2

1- Alice and Bob want to communicate with each other, and they agree to use Diffie-Hellman with prime p = 17 and generator g = 3.

(a) Alice picks a = 4 as her private key. What does she send to Bob?
(b) Bob picks b = 11 as his private key. What does he send to Alice?
(c) What is their shared secret key s? Show how Alice would compute it and how Bob would compute it.

2-Suppose you intercept a transmission between Alice and Bob, in which they agree to perform Diffie Hellman key exchange with p = 23 and g = 15. In the next message you intercept, you hear that Bob's public key is B = 3. What is Bob's private key?

3- Using RSA, choose p = 13 and q = 17, and encode the word "FLOOR" by encrypting each letter separately. Show the process of deriving n, d, e, and z. Each letter will be encrypted separately as a number between 1 and 26. Apply the decryption algorithm to the encrypted version to recover the original plaintext message. For both encryption and decryption provide a table as below to show the process:

Letter	m	m^e	ciphertext	c^d	c^d(mod N)	Decoded m
F	6					
L						
O						
O						
R						

4- Show that the following system of congruence has no solution:

$x \equiv 4 (\mathrm{mod}\ 12)$ and $x \equiv 6\ (\mathrm{mod}\ 18)$.

You can start by writing the equation for congruence ($a \equiv b(\mathrm{mod}\ c)$ → $a-b = c*t$) and then get to a contradictory result.