Tutorial 5 Solutions

1. *Describe the RSA public key encryption system and show how it works when prime numbers 5 and 7 are used to construct the modulus n = 35. Choose an encryption parameter e and calculate the corresponding decryption parameter d. Use these values to encrypt the plaintext value 17 and decrypt the resulting ciphertext to recover the plaintext.*

p = 5, q = 7, n = 35

$\phi(n) = (p-1)(q-1) = 4 * 6 = 24$

Smallest integer that does not have a common factor with 24 is 5. Choose e = 5.
Solve de = 1 (mod 24)
24 d = 24 (always true)
5 d = 1 (e is 5)
19d = 23 (subtract)
14d = 22 (subtract 5d=1)
9d = 21 (subtract 5d=1)
4d = 20 (subtract 5d=1)
d = -19 = 5 (5d=1 - 4d=20)
so d = 5.

```
P = 17

C = 17^5 % 35
  x  a  z
  1 17  5
    17  4
     9  2    17^2 = 289 =  9
    11  1     9^2 =  81 = 11
    12  0    17*11 = 187 = 12
C = 12

P = 12^5 % 35
  x  a  z
  1 12  5
    12  4
     4  2    12^2 = 144 =  4
    16  1
    17  0    12*16 = 192 = 17
```

2. *Describe in detail the Diffie-Helman method whereby Alice and Bob can agree on a common key. This protocol is vulnerable to a clogging attack.*

Alice and Bob agree on two numbers, a large prime q and a primitive root of q, alpha. They both choose a random number, X, as their private key. They calculate Y = alpha ^ X (mod q) and send the value to the other. It is hard to calculate X from Y, the discrete logarithm problem. Alice calculates YB^XA (mod q) and Bob similar, and both numbers are the same.

3. *What is a blind signature and what are the benefits of using one? Show how the RSA algorithm can be used to produce blind signatures. Give one way that the person performing the blind signature can ensure that he is not swindled.*

Alice chooses a blinding factor k and sends $M k^e$ mod n. She gets back $k M^d$ mod n and multiplies by (1/k) to remove the blinding factor and recover the signed message. (e, d, n) are Bobs keys.

The signer does not know what he is signing, and can use the cut and choose algorithm. The person wanting a document signed prepares a number of equally useful but different documents for blind signature. They are all signed, and then the signer asks for the blinding factors of all but one of the documents. He can then verify that all these documents are acceptable, and so assumes that the one he has not seen is also acceptable.