Nathan Lutz

Dr. Wahab

Assignment 5

***Q1:***

Assume each individual digit of a message M= 1020304 is encrypted with**K**=3.

What is the value of the resulting cipher assume we are using:

A.   Mod **5** addition

Answer: 4303132

B.    Mod **5** multiplication

Answer: 3010402

**C.**    Mod **5** exponentiation  
 Answer: 1040204

***Q2:***

A.     Verify that **d=<65, 133>** is the corresponding private key of**e=<5, 133>**.

Let's say m = 22.

First we sign; s = 225 mod 133 = 15.

Then we verify; s = 15, m = 1565 mod 133 = 22.

The two are a private/public key pair.

B.     Use the efficient exponentiation scheme described in RSA to encrypt a message **M = 100**.

Select primes p=17, q=23.

n = pq = 17.23 = 391  
Ø = (p-1)(q-1) = 16.22 = 352

Choose e=5  
Check gcd(e, p-1) = gcd(5, 16) = 1   
and check gcd(e, q-1) = gcd(5, 22) = 1  
therefore gcd(e, Ø) = gcd(e, (p-1)(q-1)) = gcd(5, 352) = 1

Compute d such that ed ≡ 1 (mod Ø)  
compute d = e-1 mod Ø = 5-1 mod 352  
find a value for d such that Ø divides (ed-1)  
d = .2

Public key = (n, e) = (391, 5)  
Private key = (n, d) = (391, .2).

message m = 100, c = me mod n = 1005 mod 391 = 10000000000 mod 391 = 223.

***Q3:***

Assume that ***A*** and***B***, and ***C*** are using Diffie-Hellman with  ***p***=19 and***g*** = 7.

Let  ***SA*** = 11 and ***SB*** = 13, and ***SC*** = 17.

In order to avoid the man-in-the-middle attack, they deposit their public values ***PA*** , ***PB***  and ***PC***with a ***trusted authority*** (***TA***).

1. Compute the public values ***PA ,PB***and***PC***

Answer: PA = 7^11 mod 19 = 11, PB = 7^13 mod 19 = 7, PC = 7^17 mod 19 = 11­

1. Compute the shared secret between each pair of these individuals based on the values deposited with the ***TA***

KAB = 7^11 mod 19 = 11

KBC = 17^13 mod 19 = 7

PAC = 7^11 mod 19 = 11