Michael Chillemi

12/8/2021

Homework – 7

Cryptography

1. Determine the order of all elements of the following multiplicative groups:

•

•

•

Identify which elements are the generators for the respective groups.

ANSWER:

* G = = {1,2,3,4,5}, mod 5

, ,

, O(2) = 4

O(3) = 4

O(4)=2

G = <3>

* G = = {1,2,3,4,5,6}, mod 7

1 = 1

O(1) = 1

O(2) = 3

O(4) = 3

O(5) = 6

O(6) = 2

G = <3>,<5>

* G = = {1,2,3,4,5,6,7,8,9,10,11,12}, mod 13

O(1) = 1

O(2) = 12

O(3) = 2

O(4) = 6

O(5) = 4

O(6) = 12

O(7) =12

O(8) = 4

O(9) = 3

O(10) = 6

O(11) = 12

O(12) = 2

G = <2>,<6>,<7>,<11>

2. Compute the two public keys and the common key for Diffie-Hellman key exchange

scheme in with the following parameters:

• 𝛼 = 2, 𝑝 = 467, 𝑎 = 3, 𝑏 = 5

Here, 𝛼 is the primitive element or the generator, 𝑎 and 𝑏 are respectively the private

keys of Alice and Bob.

ANSWER:

P = 467

Private key of Alice = a = 3

Private key of Bob = b = 5

Public key of Alice

Public key of Bob

Session Keys

Secret Key = 78

3. Show the steps of computing the fast exponentiation with Square-and-Multiply

algorithm for the following exponentiations:

•

•

•

ANSWER:

4. Implement the Square-And-Multiply algorithm, which is used for fast exponentiation

in Public Key cryptography. Your method should take three inputs:

a. The base element 𝑋

b. The exponent 𝑒

c. The modulus 𝑛

The method should return the value of 𝑚𝑜𝑑 𝑛.