**Jeremy Barthélemy  
ECE 746  
Hw. 7**

1.

a. m = roof(sqrt(|G|)) = roof(sqrt(|2163|)) = 282  
Storage Requirement = m \* 2 \* roof(log2 O), where O = 2163 🡪  
Storage Requirement = 282 \* roof(log2 2163) 🡪 1.97055\*1026 = dividing by 240 🡪 1.7922\*1014TB   
b. Cost = 1.7922\*1014TB \* $100 = 1.7922\*1016  
c. Taking (log2 (cost/1,000,000)) = 34.06 🡪 this will take over 34 \* 18 months = approximately 51 years!

2.  
Z109, m = roof(sqrt(108)) = 11  
mu = alpha^-im = 6^-11 mod 109 = (6^11)^-1 mod 109 = 14 mod 109

|  |  |
| --- | --- |
| j | alpha^j |
| 0 | 1 |
| 1 | 6 |
| 2 | 36 |
| 3 | 107 |
| 4 | 97 |
| 5 | 37 |
| 6 | 4 |
| 7 | 24 |
| 8 | 35 |
| 9 | 101 |
| 10 | 61 |

a.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| a^j | j |  | Yi = beta \* alpha^-im | i |
| 1 | 0 |  | 98 | 0 |
| 4 | 6 |  | 64 | 1 |
| 6 | 1 |  | 24 | 2 |
| 24 | 7 |  | 9 | 3 |
| 35 | 8 |  | 17 | 4 |
| 36 | 2 |  | 20 | 5 |
| 37 | 5 |  | 62 | 6 |
| 61 | 10 |  | 105 | 7 |
| 97 | 4 |  | 53 | 8 |
| 101 | 9 |  | 88 | 9 |
| 107 | 3 |  | 33 | 10 |

After making the tables, we match the respective values(in bold) and find:a = j0 + i0m = 7 + 2\*11 = 29  
  
b.   
We do the same lookup but for the case with beta = 99:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| a^j | j |  | Yi = beta \* alpha^-im | i |
| 1 | 0 |  | 99 | 0 |
| 4 | 6 |  | 78 | 1 |
| 6 | 1 |  | 2 | 2 |
| 24 | 7 |  | 28 | 3 |
| 35 | 8 |  | 65 | 4 |
| 36 | 2 |  | 38 | 5 |
| 37 | 5 |  | 96 | 6 |
| 61 | 10 |  | 36 | 7 |
| 97 | 4 |  | 68 | 8 |
| 101 | 9 |  | 80 | 9 |
| 107 | 3 |  | 30 | 10 |

a = j + im = 2 + 7\*11 = 79

3.  
m = 4  
Finding pairs for j index:

|  |  |  |  |
| --- | --- | --- | --- |
| j | a^j | base2 | base10 |
| 0 | 1 | 1 | 1 |
| 1 | x^2 | 100 | 4 |
| 2 | x+1 | 11 | 3 |
| 3 | x^3+x^2 | 1100 | 12 |

|  |  |
| --- | --- |
| a^j | j |
| 1 | 0 |
| x+1 | 2 |
| x^2 | 1 |
| x^3+x^2 | 3 |

Yi = β\*α-im

µ = α-m = x3 + x + 1

y0 = β \* α0 = x3 + x

y1 = β \* µ = x

y2 = β \*µ^2 = x2+1

y3 = β \*µ^3 = 1

j0 = 0, i0 = 3

a = j0 + i0\*m = 12

4.

|  |  |  |
| --- | --- | --- |
| alpha | beta | p |
| 25 | 6 | 47 |

|  |  |  |
| --- | --- | --- |
| a | b | x |
| 1 | 1 | 9 |
| 2 | 1 | 37 |
| 2 | 2 | 34 |
| 2 | 4 | 2 |
| 2 | 6 | 25 |
| 2 | 8 | 7 |
| 2 | 10 | 17 |
| 4 | 1 | 1 |
| 4 | 2 | 6 |
| 4 | 4 | 28 |
| 4 | 6 | 21 |
| 4 | 8 | 4 |
| 4 | 10 | 3 |
| 6 | 1 | 14 |
| 6 | 2 | 37 |
| 6 | 4 | 16 |
| 8 | 1 | 8 |
| 8 | 2 | 1 |

Looking at the required criteria, we find these to be satisfactory:

|  |  |  |
| --- | --- | --- |
| a | b |  |
| 4 | 1 | 1 |
| 8 | 2 | 1 |

We thus compute:

(b1-b2)^-1 \* (a2-a1) mod O = z

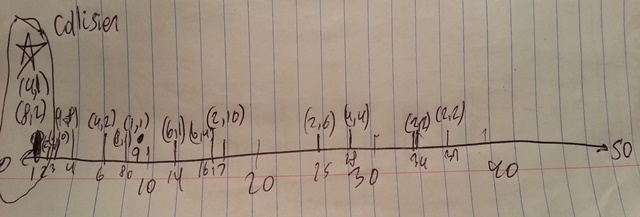
(-1)^-1 \*(4) mod 23 = z

22^-1 \* 4 mod 23 = z

z 19

We verify that with 2519 == 6 mod 47

5.

****

6.   
α = 2  
β = 278  
p = 467  
We must determine z with relation to the equation of : αz = β mod p by using Index Calculus:  
2z = 278 mod 467  
  
We do this by taking α to a variety of exponents in the hopes of obtaining a result as a combination of the products of elements of our factor base mod p:

225 mod 467 = 15 = 3\*5  
2116 mod 467 = 32 \* 7  
2283 mod 467 = 2 \* 112

251 mod 467 = 2 \* 32 \* 52  
247 mod 467 = 26 \* 5

2101 mod 467 = 2 \* 33 \* 7  
  
For the factor base:  
{2, 3, 5, 7, 11}  
We assign L2, L3, L5, L7, and L11 to perform the following computations based upon the above:  
  
L3 + L5 = 25

L3 + L7 = 116

L2 + 2L11 = 283

L2 + 2L3 = 2L5 = 59

6L2 + L5 = 47

L2 + 3L3 + L7 = 101

Solving the matrices,

L3 = 450

L5 = 41

L7 = 148

L11 = 141

β\*αk = 278\*16 mod 467 = 245 = 5\*72

log2278 = log25 + log27 - 4 mod 467 = 333

7.

Provided that an attacker is able to obtain the exponent z using index calculus for a given key exchange system for a single user, he will also be able to do the same for all other users, as he will have α, β, and p all readily available. I would recommend the use of at least 300 bits for p to provide strong security, as the DL problem would require a large amount of computations, even with some of the best methods.