DALHOUSIE UNIVERSITY

Network Security (CSCI-6708)

Assignment - 8

Shivam Gupta
B00810723

Question 1.

a) P=11
G=13

Let's say,
SA=4
SB=5

TA= g^SA mod p
TA= 13^4 mod 11
TA= 16mod 11
TA=5

TB= g^SB mod p
TB= 13^5mod11
TB= 10

KEY= TB^SA mod p = 10^4 mod 11
= 10x10x10x10 mod 11
= 1

KEY= TA^SB mod p= 5^5 mod 11
= 5x5x5x5x5 mod 11
= 1
Thus,
Key= 1

b) P=7
G=17
SA=4
SB=5
TA= g^SA mod p
TA= 17^4 mod 7
TA= 4 mod 7
TA=4

TB= g^SB mod p
TB= 17^5mod7
TB= 5

KEY= TB^SA mod p = 5^4 mod 7
= 5X5X5X5 mod 7
= 2

KEY= TA^SB mod p= 4^5 mod 7
= 4x4x4x4x4 mod 7
= 2
Thus,
Key= 2

c) P=17
G=13
SA=4
SB=5
TA= g^SA mod p
TA= 13^4 mod 17
TA= 13x13x13x13 mod 17
TA=1

TB= g^SB mod p
TB= 13^5mod 17
TB= 13

KEY= TB^SA mod p = 13^4 mod 17
= 13x13x13x13 mod 17
= 1

KEY= TA^SB mod p= 1^5 mod 17
= 1x1x1x1x1 mod 17
= 1
Thus,
Key= 1