Ryan Young

CSE 3400

3/27/2020

Homework 6

1.) *Use Fermat's Little Theorem to find 22^{-1} in multiplicative group Z^*_{101}. Note that 101 is prime. Please show the steps to find the answer. The number of multiplications (and squaring) operations should be less than 14 and the operations are always on numbers less than 101.*
Since this question is asking about the multiplicative group we can use the form of Fermat's Little Theorem: $a^{p-1} = 1 (\text{mod } p)$
   1. 22^{101-2} mod 101 -> 22^{99} mod 101 -> $22^{64+32+2+1}$ mod 101
   2. $22^{64+32+2+1}$ mod 101 -> $22^{64} * 22^{32} * 22^{2} * 22^{1}$ mod 101
   3. **22^{1} mod 101** = 22, **22^{2} mod 101** = 80, **22^{4} mod 101** = $(22^2)^2$ mod 101 = $(80)^2$ mod 101 = 37, **22^{8} mod 101 = $(22^4)^2$** mod 101= $(37)^2$ mod 101= 56, **22^{16} mod 101** = $(22^8)^2$ mod 101 = $(56)^2$ mod 101 = 5, **22^{32} mod 101** = $(22^{16})^2$ mod 101 = $(5)^2$ mod 101 = 25, and **22^{64} mod 101** = $(22^{32})^2$ mod 101 = $(25)^2$ mod 101 = 19.
   4. 19 * 25 * 80 * 22 mod 101 = 836,000 mod 101 = 23

2.) *Use (extended) Euclidean algorithm to find 38^{-1} in multiplicative group Z^*_{85}.*
Find the inverse of 38 in 1 – 84.
Gcd(38, 85) = 1 because they are coprime
85 – 38(2) = 9
38 – 9(4) = 2
9 – 2(4) = 1
Proof that they are coprime
Extended:
9 = 85 - 38(2)
2 = 38 – 9(4)
1 = 9 – 2(4)
1 = 9 – (38 – 9(4))(4) -> 1 = 9 – 38(4) – 9(16)
1= 9 – 38(4) – 9(16) -> 1 = 85 - 38(2) -38(4) + 85(16) - 38(32)
85(17) – 38(38) Choosing the second coefficent
So, the inverse is -38 mod 85 which is 47! Double checking this we can see that |-38|*47 mod 85 = 1!

3.) *Show that 15 is a generator of the multiplicative group Z^*_{23}. Then find the smallest positive integer x such that $15^x = 5$.*
We know that the multiplicative group z^*_{23} has 22 elements and that the elements that are not the generator will be powers of the generator. The set should be 1 through 22 because zero has to be excluded in order to form a group because you cannot divide by 0. To prove 15 is a generator for the group Z^*_{23} I will show that 15 can produce all the numbers in the set.

15 * 1 mod = 15
15 * 2 mod = 7
15 * 3 mod = 22
15 * 4 mod = 14

15 * 5 mod = 6
15 * 6 mod = 21
15 * 7 mod = 13
15 * 8 mod = 5
15 * 9 mod = 20
15 * 10 mod = 12
15 * 11 mod = 4
15 * 12 mod = 19
15 * 13 mod = 11
15 * 14 mod = 3
15 * 15 mod = 18
15 * 16 mod = 10
15 * 17 mod = 2
15 * 18 mod = 17
15 * 19 mod = 9
15 * 20 mod = 1
15 * 21 mod = 16
15 * 22 mod = 8

This means that 15 is a generator in the group and that x = 8!

4.) *Alice and Bob share master key MK and perform authenticated DH protocol daily, at the beginning of every day I, to set up a 'daily key' k_i for day i. Assume that Mal can eavesdrop on communication between Alice and Bob every day, but perform Man in the Middle Attacks only every even day(I s.t. I =0(mod 2). Assume further that Mal is given the master key MK, on the fifth day. Could Mal decipher message sent during day I, for I = 1, …., 10? Write your response in a table.*

Day	Attacker Capabilities	Adversary Actions	Can the Attacker Decipher?
Day 1	Eavesdropping	Sees: g^{ai} mod p, g^{bi} mod p, p and g are public information	No, does not know a_i, b_i and the MK
Day 2	Man in the Middle	Sees: g^{ai} mod p, g^{bi} mod p, ai, bi p and g are public information	No, does not know the MK
Day 3	Eavesdropping	Sees: g^{ai} mod p, g^{bi} mod p, p and g are public information	No, does not know a_i, b_i and the MK
Day 4	Man in the Middle	Sees: g^{ai} mod p, g^{bi} mod p, ai, bi p and g are public information	No, does not know the MK
Day 5	Eavesdropping and gets the MK	Sees: g^{ai} mod p, g^{bi} mod p, p and g are public information and now has MK	No, even though he or she has the MK still needs a_i and b_i!

Day 6	Man in the Middle	Sees: g^{ai} mod p, g^{bi} mod p, ai, bi p and g are public information + has MK	Yes, he or she now has the MK a_i and b_i!
Day 7	Eavesdropping	Sees: g^{ai} mod p, g^{bi} mod p, p and g are public information + has MK	No, does not know a_i, b_i
Day 8	Man in the Middle	Sees: g^{ai} mod p, g^{bi} mod p, ai, bi p and g are public information + has MK	Yes, he or she now has the MK a_i and b_i!
Day 9	Eavesdropping	Sees: g^{ai} mod p, g^{bi} mod p, p and g are public information + has MK	No, does not know a_i, b_i
Day 10	Man in the Middle	Sees: g^{ai} mod p, g^{bi} mod p, ai, bi p and g are public information + has MK	Yes, he or she now has the MK a_i and b_i!

5.) *It is proposed that to protect the DH protocol against an imposter, we add an additional 'confirmation' exchange after the protocol terminated with a shared key k=h(g^{ab} mod p). In this confirmation, Alice will send to Bob $MAC_k(g^b)$and Bob will respond with $MAC_k(g^a)$. Show the message-flow of an attack, showing how an attacker (Monster) can impersonate as Alice(or Bob). The attacker has 'MitM capabilities', i.e., it can intercept messages(sent by either Alice or Bob) and inject fake messages (incorrectly identifying itself as Alice or Bob).*

A monster performing a MitM attack will pretend to be Alice and send bob g^a mod p for some a. At the same time, it will pretend to be Bob and send Alice g^b mod p for some b. Then bob will send back g^b mod p for some b and Alice will send back g^a mod p for some a. The monster will now have a key k such that k =h(g^{ab} mod p) with both Bob and Alice. The monster can now send out the $MAC_k(g^b)$ to Bob and $MAC_k(g^a)$ to Alice and have all the information. This works because the hash function does not use any key.

6.) *Assume that there is an efficient (PPT) attacker A that can find a specific bit in g^{ab} mod p, given only g^a mod p and g^b mod p. Show that the DDH assumption does not hold for this group, i.e., that there is an efficient (PPT) attacker A that can distinguish, with significant advantage over random guess, between g^{ab} mod p and between g^x for x taken randomly from[1,...,p−1].*

We know that DDH is that an attacker cannot tell the difference between g^{ab} mod p and g^c mod p with g^{c-} mod p being random but of the same length as g^{ab} mod p. An attacker A who can find a specific bit in g^{ab} mod p, say this is the last bit. The g^a or g^b will then reveal whether a/b is even or odd. Given g^a, g^b and g^{ab}, the attacker will now have a probabilistic method to be able to tell the difference between a random group element g^c and g^{ab}.