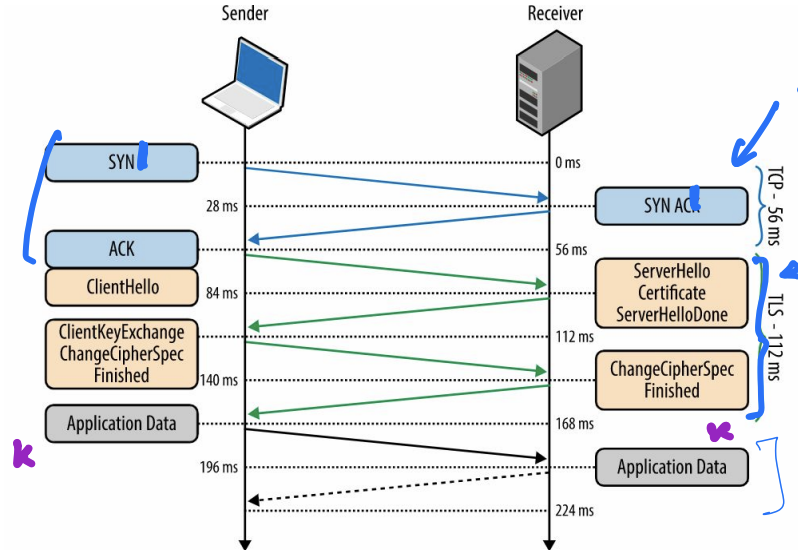
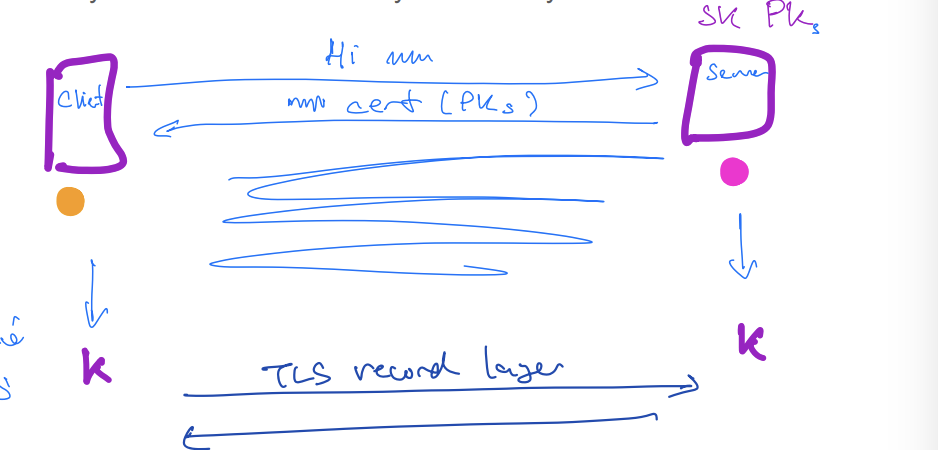
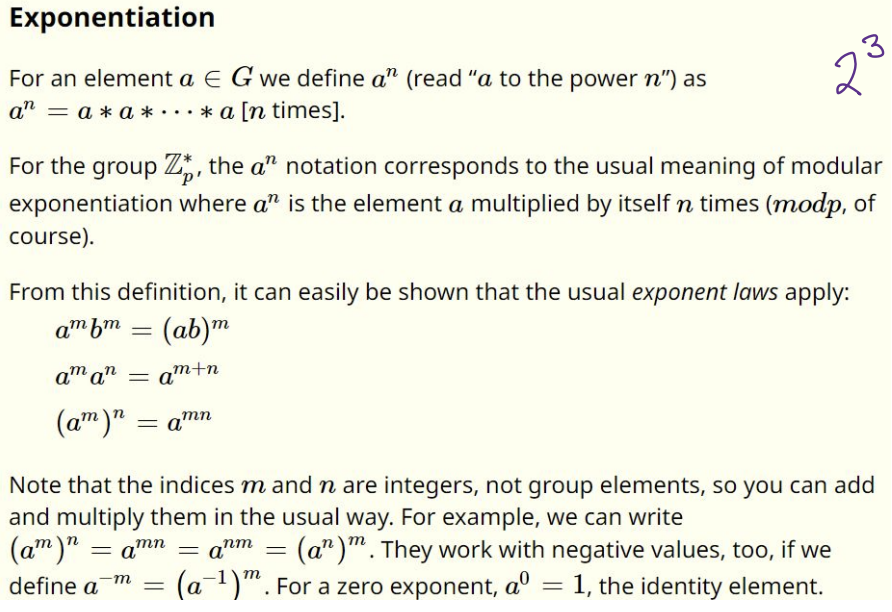
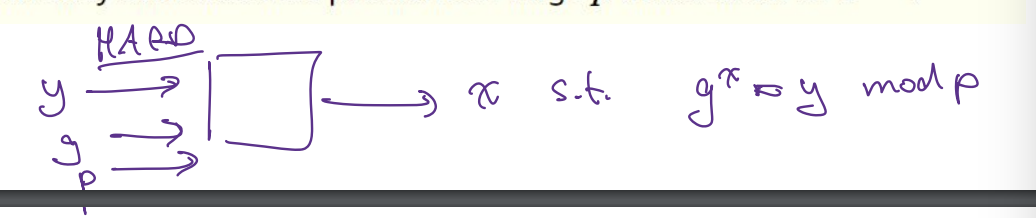
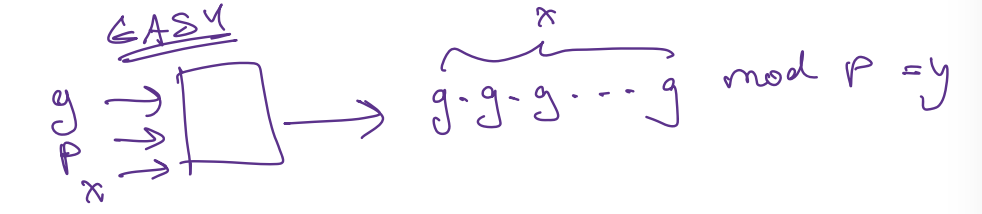
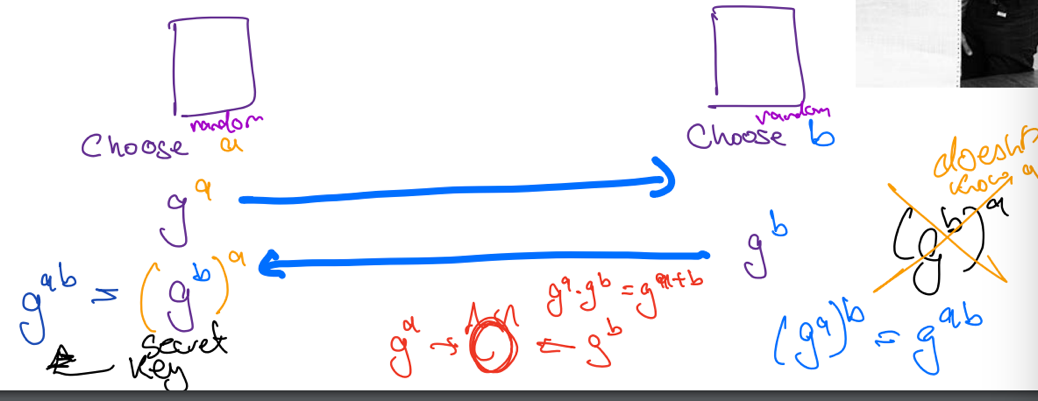
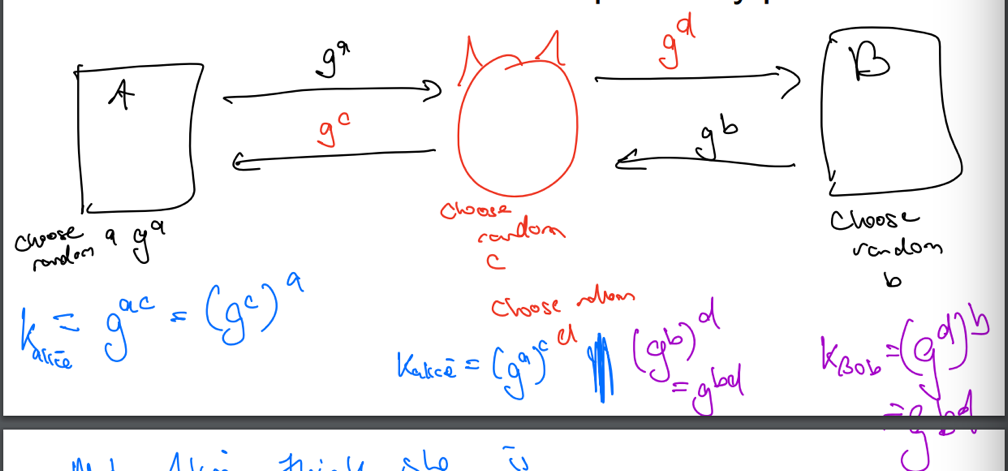
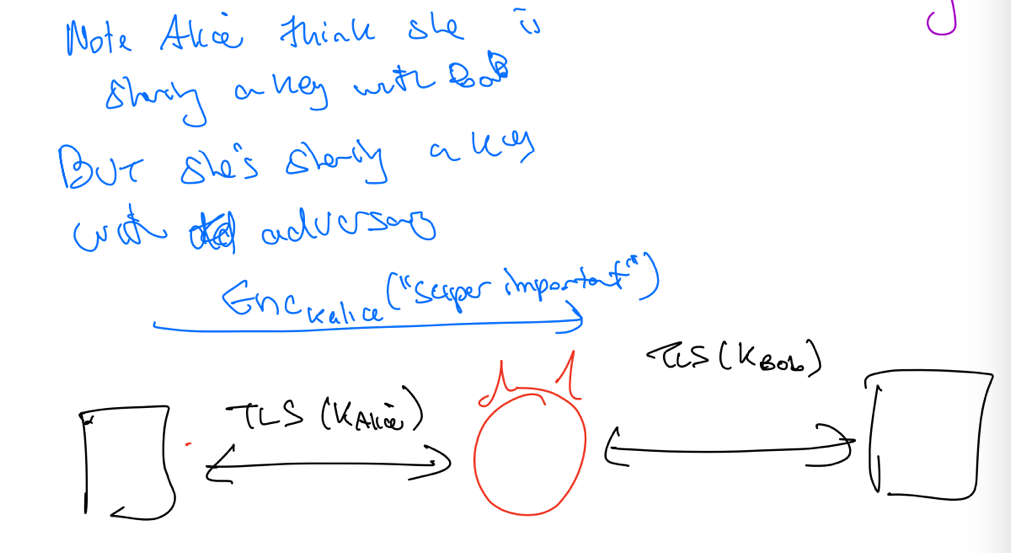
CAS CS 357

InClass Note 15

1. Sender-Receiver model
2. 
3. Start with a certificate then derive a symmetric key
4. ServerHello Certificate ServerHelloDone 🡨 TLS, Handshake
5. Application Data 🡪 TLS record layer (has keys)
6. Goal of key exchange
7. Use a public key to establish a shared symmetric key
8. 
9. Multiplicative group modulo p, where p is prime
10. The multiplicative group modulo p is the set of p-1 elements {1,2,..,p-1} under the group operation is multiplication modulo p, where p is prime
11. Let’s say p = 11
12. 2 \*3 = 6 mod 11 = 6
13. It satisfies the five axioms for an Abelian group
14. G1 Closure: any two elements in the set multiplied together modulo p give another element in the set
15. G2 Identity: the number 1 is the multiplicative identity and gives 1\*x = x = x\*1 for any x in the set
16. G3 Inverses: every element x in the set has a corresponding inverse element x-1 in the set such that x\*x-1 = 1= x-1\*x (mod p)
17. G4 Associativity: for any element a, b, c in the set, a\*(bc) = (ab)\*c (mod p)
18. G5 Commutativity: for any two elements a, b in the set, ab = ba (mod p)
19. Exponentiation
20. 
21. Generator
22. The element g is a generator of the group G if the group can be represented at G = {1, g, g^2,…g^(p-1)} and gi=gj whenever i = j (mod p)
23. In particular, gn = g0 = 1, and g-1 = gn-1
24. The Discrete Logarithm Problem (DLP)
25. The discrete logarithm problem (DLP) for Z(multiplicative group modulo p) is given g, y in Zp then find x such that y = gx mod p
26. This is currently at intractable problem for large p in the order of 21024
27. 
28. It is difficult to produce x such that gx = y mod p
29. 
30. It is easy to produce gx mod p = y
31. DHE key exchange
32. Only secure against eavesdropper
33. Everything is implied to be mod p
34. Public parameters: G is a cyclic group, g is a generator of that group
35. 
36. Diffie Hellman Key Exchange: what happens if the Man in the middle can add/drop/modify packets?
37. 
38. 
39. We need to authenticate DH exchange to prevent active attacks
40. 