Review Week 5

- Key exchange
  - 3rd party solution (TTP)
- Generating keys
  - x shared key with y
    - eavesdropping security only
    - x contains k_a
    - y contains k_b
    - eavesdropper learns nothing about k_ab
- Toy protocol
  - insecure against active attackers
    - replay attack - attack records session between x and y then replays the session to y
- Merkle Puzzle
  - key exchange without a TTP
  - puzzle
    - puzzle(P) = E(P,"message")
    - P = 0^96llb_1…b_32
    - Alice
      - prepares 2^32 puzzles
      - For i = 1 to 2 ^ 32 choose random P_i element of {0,1}^32 and x_i, k_i element {0,1} ^ 128
      - puzzle_i = E(0^96 ll P_i ll k_i)
      - send all the puzzles to Bob
    - Bob
      - choose random puzzle_j and solves it
      - obtains (x_j, k_j) and solves it
      - sends x_j to Alice
    - Alice
      - lookup puzzle with number x_j. Use k_j as shared secret
- Merkle Puzzles
  - Alice's and Bob's work O(n) each
  - Eavesdropper's work O(n^2)
- Diffie-Hellman protocol
  - Fix a large prime p
  - Fix an integer g in 1 to p
  - Alice and Bob
    - Alice choose random a in 1 to p - 1
    - Bob choose random b in 1 to p - 1
    - Alice sends A <- g^a (mod p)
    - Bob sends B <- g^b (mod p)
    - Shared key = k_ab = g^ab (mod p)
  - Eavesdropper sess: p, g, A, and B
    - DH(g^a,g^b) = (g^ab) mod p
    - How hard is the function to compute
- Man in the middle attack
  - DH insecure against active attacks
  - Intercept message and send own values a' and b'
- Public key encryption
  - G(): randomized algorithm outputs key pair (pk,sk)

    - E(pk,m): randomized algorithm that takes m element M and outputs c element C
    - D(sk,c): deterministic algorithm that takes c element C and outputs m element M or reject
    - Consistency
- Semantic security
    - Two experiments the probability of outputting experiment 0 = 1or experiment 1 = 1 is negligible
- Establishing a shared secret
    - Alice and Bob
        - Alice sends pk to Bob
        - Bob sends c <- E(pk,x) to Alice
        - Alice decrypts D(sk,c) -> x
    - Adversary sees pk, E(pk,x) and wants x element M
    - Semantic security
        - adversary cannot distinguish {pk, E(pk,x),x} from {pk, E(pk,x),rand element M}
    - Can derive session key from x
    - vulnerable to man in the middle
- Public key encryption: constructions generally rely on hard problems from number theory and algebra
- Number Theory see notes