Review Week 4

- CPA
- Semantic security
- Confidentiality: semantic security against a CPA attack
  - encryption secure against eavesdropping
- Existential unforgeability -
- Integrity:
  - Existential unforgeability under chosen message attack
- Authenticated Encryption
  - Two requirements
    - Semantically secure
    - Ciphertext Integrity:
      - attacker cannot create new ciphertexts that decrypt properly
  - Authenticity - attacker cannot fool bob into thinking a message was sent alice
- CTR mode -
- CBC -
- IV -
- TCP Checksum
- Active attack - modifying information that is in route
- Chosen ciphertext security (CCA is chosen ciphertext attack)
  - can obtain encryption of arbitrary messages of his choice
  - can decrypt any ciphertext of his choice, other than the challenge text
  - goal: break semantic security
- MACs
  - designed for integrity not confidentiality
  - Encrypt-then-mac
    - always provides A.E.
  - MAC - then - encrypt
    - may be insecure against CCA attacks
  - MAC security
    - cannot create a new valid tag for the same message (semantic security)
- TLS record protocol
  - decryption
    - dec(k_bs, record, ctr_bs)
    - check pad format
    - check tag on [ctr_bs ll header ll data]
- Padding oracle:
  - attacker submits cipher text and learns if last bytes of plaintext are a valid pad
  - allowed to learn something about the resulting text
  - timing attacker result of the padding oracle
- SSH binary protocol
  - attack on the length field of the packet
    - learns the length field from the packet
    - to prevent this send the length field unencrypted
    - add a mac after the length field
- Key Derivation
  - when source key is uniform use a CTX a string that uniquely identifies the application ll 0 .. n for the block
- Slow hash function

    - iterate the hash function k times
- Deterministic encryption
    - cannot be CPA secure
        - attacker can tell when when two ciphertexts encrypt the same message
- SIV (Synthetic IV)
    - CPA that doesn't use nonces has to be randomized
- EME: constructing a wide block PRP
- Deterministic authenticated encryption
    - deterministic CPA security
    - ciphertext integrity
- Disk encryption
    - encrypt sectors using a PRP
- Tweakable block ciphers
    - use sector number as the tweak => every sector gets its own independent PRP
    - security
        - did we interact with pseudo random functions or truly random functions
    - Trivial construction
        - The trivial tweakable construction
            - E_tweak(k,t,x) = E(E(k,t),x)
            - to encrypt n blocks need 2n evaluations of E(.,.)
    - XTS tweakable block cipher
        - more efficient then the trivial construction
- Format preserving encryption (FPE)
    - map given CC# to {0,…,s-1} => apply PRP to get an output in {0,….,s-1} => map output back to CC#
    - **Same security as Luby-Rackoff construction**