***Security is not an afterthought.***

***There is no security in obscurity.***

***Thou shall not develop a deterministic solution for confidentiality.***

***Thou shall only use an approved Cryptography API***

* Deterministic algorithm violates diffusion
  + Reasons
    - It isn’t random
* Example
* The input you provide today will give you the same output tomorrow if you provide the same input
* No deterministic solution can provide confidentiality.
* IV provides randomness in the encryption algorithm.
  + Counter mode is a type of IV.
  + Wi-Fi router uses counter of AES encryption.
  + IV should be changed every single time.
    - Cannot be recycled
    - Not constant
* Pre-Computation
  + Initialize IV and start encrypting it before the message even comes.
  + Just XOR when the message comes.
* Parallizable
  + Run different threads independently
* You can’t encrypt many message with one key
* GCM – Galois Counter mode
  + Combines Confidentiality and Integrity
  + The only time you’re allowed to use AES other than 256 is when you are using GCM mode.
* CTR – Counter mode
* Entropy Pool
  + Uncertain
  + Disorder
  + Entropy is represented with bits
  + A way of measuring events outside of the machine and storing it into a pool
  + Microprocessor comes with capacitor
    - Which is unpredictable so it’s a candidate for storing in entropy pool
* How often is the entry pool being filled up?
* If the entropy pool is drained, then the algorithm becomes deterministic again
* The truly 50 bits of entropy random number is stretched using a pseudo random algorithm (128-bits)
* PRNG (Pseudo Random Number Generated)
* Random function first goes to the OS and asked it for its entropy pool.
  + If adversary knew entropy pool at the time he uses it, then that becomes a truly random number.
  + One time pad is theoretically unbreakable
* Stream Cipher
  + How to encrypt as data come?
    - Use Counter Mode
    - You can encrypt even before the data comes
* Lack of integrity means that an adversary can tamper with encrypted data without detection.
* Integrity
  + Being able to detect attacks to message
  + You want integrity regardless of confidentiality
* Confidentiality
  + Being able to hide message