Advanced Cryptography and PKI

Three characteristics of *key strength*:

- randomness
- length of key
- cryptoperiod - expiration

  Need to explore about half of keyspace in order to break

Block Cipher Modes of Operation

- Electronic Code Block (ECB)
- Cipher Block Chaining (CBC)
- Counter (CTR)
- Galios / Counter (GCM)