Eric Altenburg **CS-306** **September 22, 2020**

Lecture 3 - Perfect Secrecy

1. Perfect correctness
   - For any k ∈ K, m∈ M and any cipertext c output of $Enc_k(m)$, it holds that $Pr[Dec_k(c) = m] = 1$
2. Towards defining perfect security
   - Defining security for an encryption scheme is not trivial
   - 3 sources of randomness:
     - generating message
     - choosing key
     - whatever randomness is being used in the probabilistic encryption
3. Attempt 1: Protect the key k!
   - Security means that
     - the adversary should **not** be able to **compute the key k**
   - Wrong: maybe C (ciphertext) isn't secure and if they can get a hold of C, then they can get the message
     - what if $Enc_k(m) := m$
4. Attempt 2: Don't learn m!
   - Security means that
     - the adversary should not be able to compute the message m
   - Wrong: difference between knowing m (message) verbatim and inferring part of m (they can still get an idea of what the message was)
     - If the scheme protects part of m, the part that's not protected could leak and ruin m
5. Attempt 3: Learn nothing!
   - Security means that
     - the adversary should not be able to learn any information about m
   - Problem with this is that it ignores the adversary's prior knowledge on m
     - Attacker may know something about m, therefore, it's nearly impossible for them to not learn **any** information about m
6. Attempt 4: Learn nothing more!
   - Security means that
     - the adversary should not be able to learn any additional information on m
   - Even if they know something about m, nothing additional from that point on is learned about m through C
   - INCLUDE
   - Nothing in Eve's knowledge of M changed before or after the message was encrypted
7. Two equivalent views of perfect secrecy
   - a posteriori = a priori
     - For every D_M, $m \in M$ and $c \in C$, for which $Pr[C = c] > 0$, it holds that $PR[M = m|C = c] = Pr[M = m]$
   - C is independent of M
     - For every m, $m' \in M$ and $c \in C$, it holds that $Pr[Enc_k(m) = c] = Pr[Enc_k(m') = c]$
       - Equally likely that c hides m but also likely that c hides another message m' that is different from m
   - Both are basically the same at capturing the idea of perfect secrecy

Lecture 3.1 - The one-time pad

1. A perfect cipher
    - A type of "substitution" cipher that is "absolutely unbreakable"
        - substitution cipher
            * individually replace plaintext characters with shifted ciphertext characters
            * independently shift each message character in a random number
                · to encrypt a plaintext of length n, use n uniformly random keys $k_1, ..., k_n$