Week 2 Notes

Uday Manchanda

October 26, 2019

Abstract

Week 2 Notes in the Coursera Course on Cryptography

1 Block Ciphers

1.1 Overview

- Crypto work horse
  - Block ciphers have two algorithms: E(Encryption) and D(Decryption)
  - n bits plaintext input and n bits ciphertext output
  - Examples
    - 3DES. n=64 bits, k=168bits
    - AES. n=128bits, k=128,192,256bits
- Built by iteration
  - Key is expanded from k_1 to k_n
  - for each k_i, a function $R(k, m)$ (a round function) is applied to the key
  - basically you iteratively the message over and over again until you get to the ciphertext
  - final output is the ciphertext
- PRPs and PRFs
  - PRF: Pseudo Random Function, defined over (K,X,Y)
  - K=keyspace, X=inputspace, Y=outputspace
  - $F : F \times X \rightarrow Y$
  - an efficient algorithm to evaluate $F(k, x)$
  - PRP: Pseudo Random Permutation defined over (K,X)
  - $E : K \times X \rightarrow X$

  - such that:
    * There exists an efficient deterministic algorithm to evalulate E(k,x)
    * The function E(k,.) is one-to-one
    * There exists an efficient inversion algorithm D(k,y)

- PRP Examples
  - AES: $K \times X \rightarrow X$ where $K = X = \{0,1\}^{128}$
  - 3DES: $K \times X \rightarrow X$ where $X = \{0,1\}^{64}, K = \{0,1\}^{168}$
  - Any PRP is also a PRF
  - A PRP is a PRF where X=Y and is efficiently invertible

- Secure PRFs
  - Let $F : K \times X \rightarrow Y$ be a PRF
  - Funs[X,Y] is the set of all functions from X to Y
  - $S_F = \{F(k,.) \text{ s.t. } k \in K\} \subseteq Funs[X,Y]$
  - A PRF is secure if:
    * a random function in Funs[X,Y] is indistinguishable from a random function in S_F
  - Size of S_F = Size of $|K|$
  - size of $Funs[X,Y]$ = Size $|Y|^{|X|}$
  - For AES it would be $2^{128 \times 2^{128}}$
  - If an adversary were to try and break the system he would either get the random function or pseudo-random function
  - The goal is to make everything look as truly random as possible

- Question
  - Assume we have a secure PRF ($F : K \times X \rightarrow \{0,1\}^{128}$)
  - Build a new PRF called G, defined as follows:
  - $G(k,x) =$
$$\begin{cases} 0^{128} & \text{if x = 0 and} \\ F(k,x) & otherwise \end{cases}$$
  - Is G a secure PRF? No
  - All the adversary has to do is query the function at x=0

- PRF $\rightarrow$ PRG
  - Let $F : K \times \{0,1\}^n$ be a secure PRF
  - Then the following $G : K \rightarrow \{0,1\}^{nt}$ is a secure PRG
  - t blocks of n bits each
  - $G(k) = F(k,0)||F(k,1)||...||F(k,t)$, counter mode
  - We took the key bit and expanded it n times by t bits

1.2 Data Encryption Standard

- test