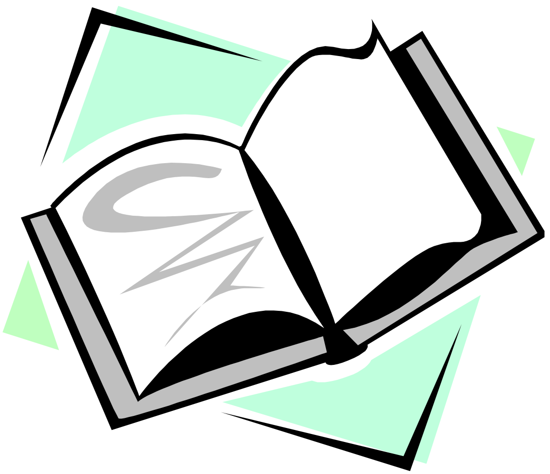
Cryptography
CS 555

Topic 8: Pseudorandom Functions and CPA Security

Outline and Readings

- Outline
  - Keyed Function
  - Pseudorandom function (PRF)
  - Encryption using PRF
  - Pseudorandom Permutation (PRF)



- Readings:
  - Katz and Lindell: 3.6.1 ~ 3.6.3

Keyed Function

- A key function F: $\{0,1\}^k \times \{0,1\}^* \to \{0,1\}^*$
  - Takes two inputs, first called the key, second input
  - When k is fixed, F_k: $\{0,1\}^* \to \{0,1\}^*$
  - We say F is length-preserving when $|F_k(x)| = |x| = |k|$
- Informal: A keyed function F is pseudorandom, iff when $k \leftarrow \{0,1\}^n$ the resulting function is indistinguishable from a function chosen at uniform random from all functions $\{0,1\}^* \to \{0,1\}^*$

Use Func_n: The Set of All Functions $\{0,1\}^* \rightarrow \{0,1\}^*$

- How large is the set Func_n? $(2^n)^{2^\wedge n} = 2^{n2^\wedge n}$
  - When n=2, this is 2^8 ; n=8, this is 2^{2048}.
- Func_n can be viewed as a big look-up table, storing values for each string in $\{0,1\}^n$
  - The table can then be viewed as a string of length $n2^n$
  - Can define a keyed function such that each key selects a function in Func_n ; call this the Random Function.
- How to implement a function f that is randomly chosen from Func_n ?
  - Maintains a table that is initially empty. When one queries f(x), first looks in the table, if x does not exist, randomly chooses y, add (x,y) to the table, and return y; if (x,y) exists, then return y.

Properties of Random Functions

- Let R be the random function such that R_k, when k randomly chosen, gives a random function in $Func_n$
  - Knowing $R_k(a)$ gives absolutely no information about $R_k(b)$ for $a \neq b$
- How to use the random function R for encryption?
  - How about $Enc_k(m)=R_k(m)$?
- Correct way: Given message m, randomly chooses r, then $c := \langle r, R_k(r) \oplus m \rangle$
  - So long as r does not repeat, no information is leaked about m
  - Assuming sharing an (extremely) long random string, different portions are used to encrypt different messages

Pseudorandom Function (PRF) Definition 3.23

- Given an efficient, length-preserving key function F: $\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^*$, we say F is a pseudorandom function iff for all PPT distinguisher D, there exists a negligible function *negl* such that

$$|\Pr[D^{F_k(\cdot)}(1^n)=1] - \Pr[D^{f(\cdot)}(1^n)=1]| \leq \mathit{negl}(n)$$

  - Where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random and f is chosen uniformly at random from Func_n.
  - D is given oracle access to a function, and needs to tell whether the function is a random one, or one from F.

An Encryption Scheme Using PRF

- Construction 3.24, using a PRF F
  - **Enc**$_k$(m): $c := \langle r, F_k(r) \oplus m \rangle$
    - where $r \leftarrow \{0,1\}^n$ is chosen at uniform random
  - **Dec**$_k$(c): given $c = \langle r, s \rangle$, $m := F_k(r) \oplus s$
  - Intuitively this is secure: so long as r is not used for different messages, $F_k(r)$ should look completely random, hence m is like being encrypted using OTP

- Theorem 3.25. If F is PRF, then Construction 3.24 is CPA-scure

Proof of Theorem 3.25

- Given any A that breaks CPA-security of Π construction 3.24, construct a distinguisher D as follows:
  - D is given oracle access to a function g, and needs to tell from which distribution is g drawn
  - When A requests an encryption, uses $c := \langle r, g(r) \oplus m \rangle$
  - If A succeeds in guessing which of m_0 and m_1 is encrypted under the challenge ciphertext, outputs 1 (PRF), otherwise output 0 (Random)

More on Proof

- When D is given a random function f
  - $\Pr[D^{f(\cdot)}(1^n)=1] = \Pr[\mathbf{PrivK}^{\mathbf{cpa}}_{\mathbf{A},\Lambda}=1] \leq ½ + q(n)/2^n$
  - Assuming that A makes at most q(n) requests for encryption,
  - We use Λ to denote Construction 3.24 with random function
  - When r used in the challenge message does not appear in other messages, $\Pr[\mathbf{PrivK}^{\mathbf{cpa}}_{\mathbf{A},\Lambda}=1] = ½$
  - Prob that r appears in other challenges is $q(n)/2^n$
- When D is given a pseudorandom function
  - $\Pr[D^{F_k(\cdot)}(1^n)=1] = \Pr[\mathbf{PrivK}^{\mathbf{cpa}}_{\mathbf{A},\Pi}=1]$
- Thus
  - $\Pr[\mathbf{PrivK}^{\mathbf{cpa}}_{\mathbf{A},\Pi}=1] > ½ + \mathrm{negl}(n)$ if and only if
    $|\Pr[D^{F_k(\cdot)}(1^n)=1] - \Pr[D^{f(\cdot)}(1^n)=1]| > \mathrm{negl}(n)$

Pseudorandom Permutations (PRP)

- We say that a length-preserving keyed function F: $\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^*$, is a keyed permutation if and only if each F_k is a bijection
- A Pseudorandom Permutation (PRP) is a keyed permutation that is indistinguishable from a random permutation
- A Strong PRP is a keyed permutation is indistinguishable from a random permutation when the distinguisher is given access to both the function and its inverse

- We assume block ciphers are PRP.

Coming Attractions …

- Block Cipher Construction
- Reading: Katz & Lindell: 5.1,5.2,5.3