CS255: Winter 2009

PRPs and PRFs

1. Abstract ciphers: PRPs and PRFs,
2. Security models for encryption,
3. Analysis of CBC and counter mode

Dan Boneh, Stanford University

PRPs and PRFs

- Pseudo Random Function (**PRF**) defined over (K,X,Y):

  $F: K \times X \rightarrow Y$

  such that exists "efficient" algorithm to evaluate F(k,x)

- Pseudo Random Permutation (**PRP**) defined over (K,X):

  $E: K \times X \rightarrow X$

  such that:

  1. Exists "efficient" algorithm to evaluate E(k,x)
  2. The function $E(k, \cdot)$ is one-to-one
  3. Exists "efficient" inversion algorithm D(k,x)

Running example

- Example PRPs: 3DES, AES, …

  AES: $K \times X \rightarrow X$ where $K = X = \{0,1\}^{128}$

- Functionally, any PRP is also a PRF.
  - A PRP is a PRF where X=Y and is efficiently invertible.