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

  DES: $K \times X \rightarrow X$ where $X = \{0,1\}^{64}$, $K = \{0,1\}^{56}$

  3DES: $K \times X \rightarrow X$ where $X = \{0,1\}^{64}$, $K = \{0,1\}^{168}$

- Functionally, any PRP is also a PRF.
  - A PRP is a PRF where X=Y and is efficiently invertible
  - A PRP is sometimes called a ***block cipher***

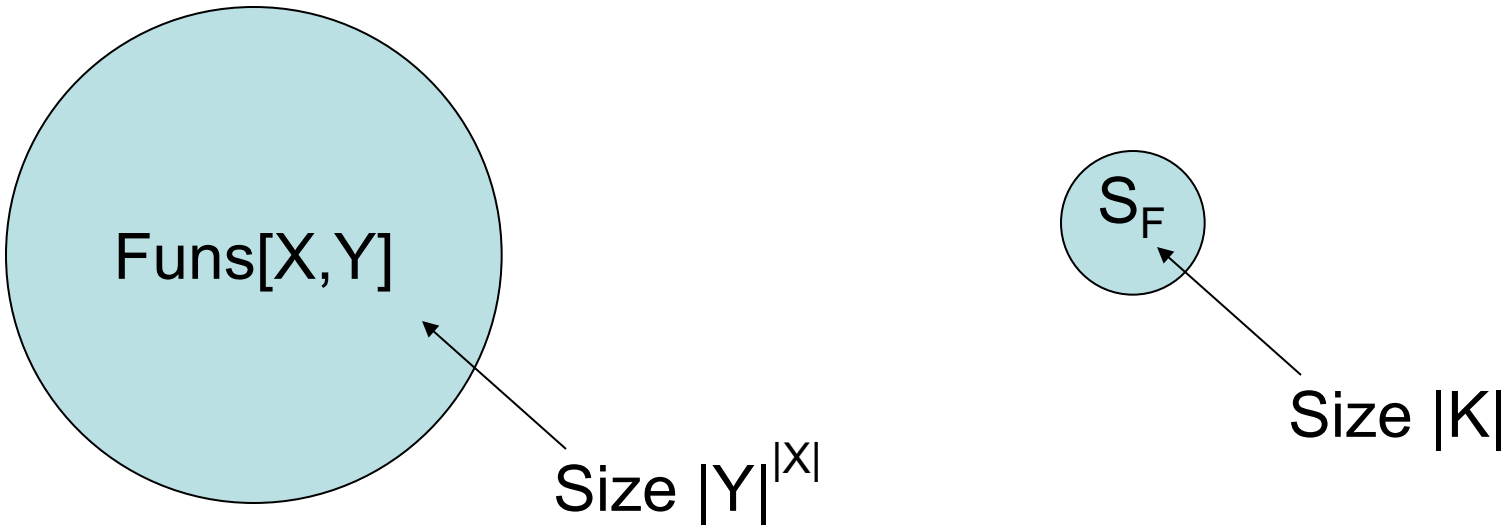
Secure PRFs

- Let $F: K \times X \rightarrow Y$ be a PRF

  Funs[X,Y]: the set of **all** functions from X to Y

  $S_F = \{ F(k,\cdot) \text{ s.t. } k \in K \} \subseteq$ Funs[X,Y]

- Intuition: a PRF is **secure** if
  a random function in Funs[X,Y] is indistinguishable from
  a random function in S_F



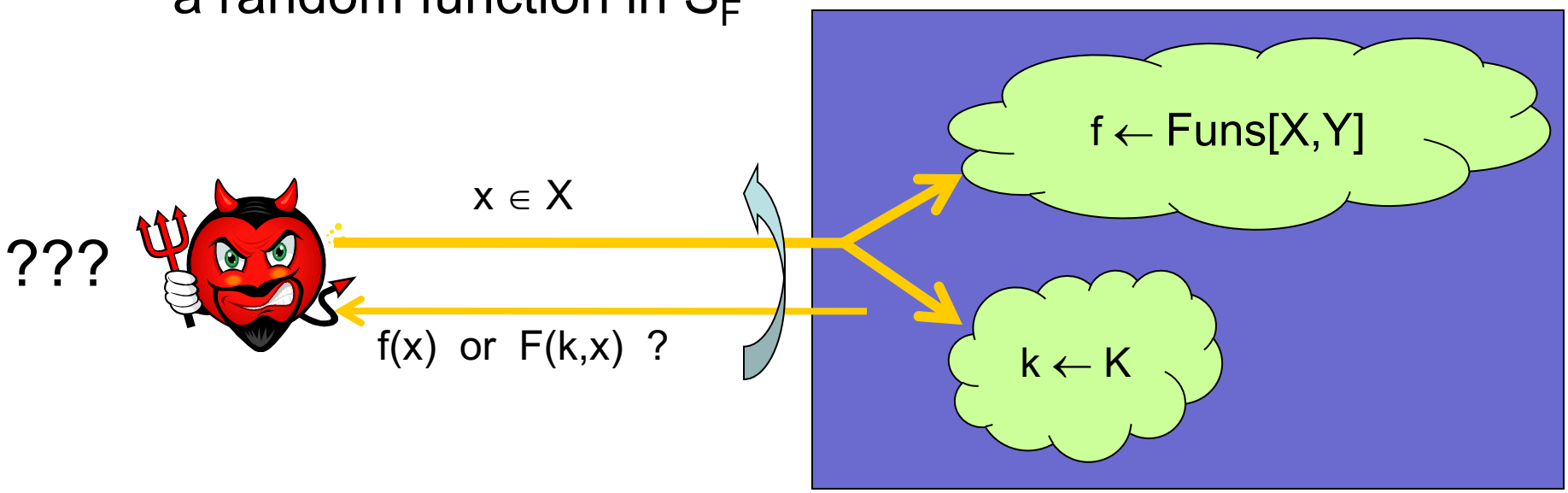
Secure PRFs

- Let $F: K \times X \rightarrow Y$ be a PRF

  Funs[X,Y]: the set of **all** functions from X to Y

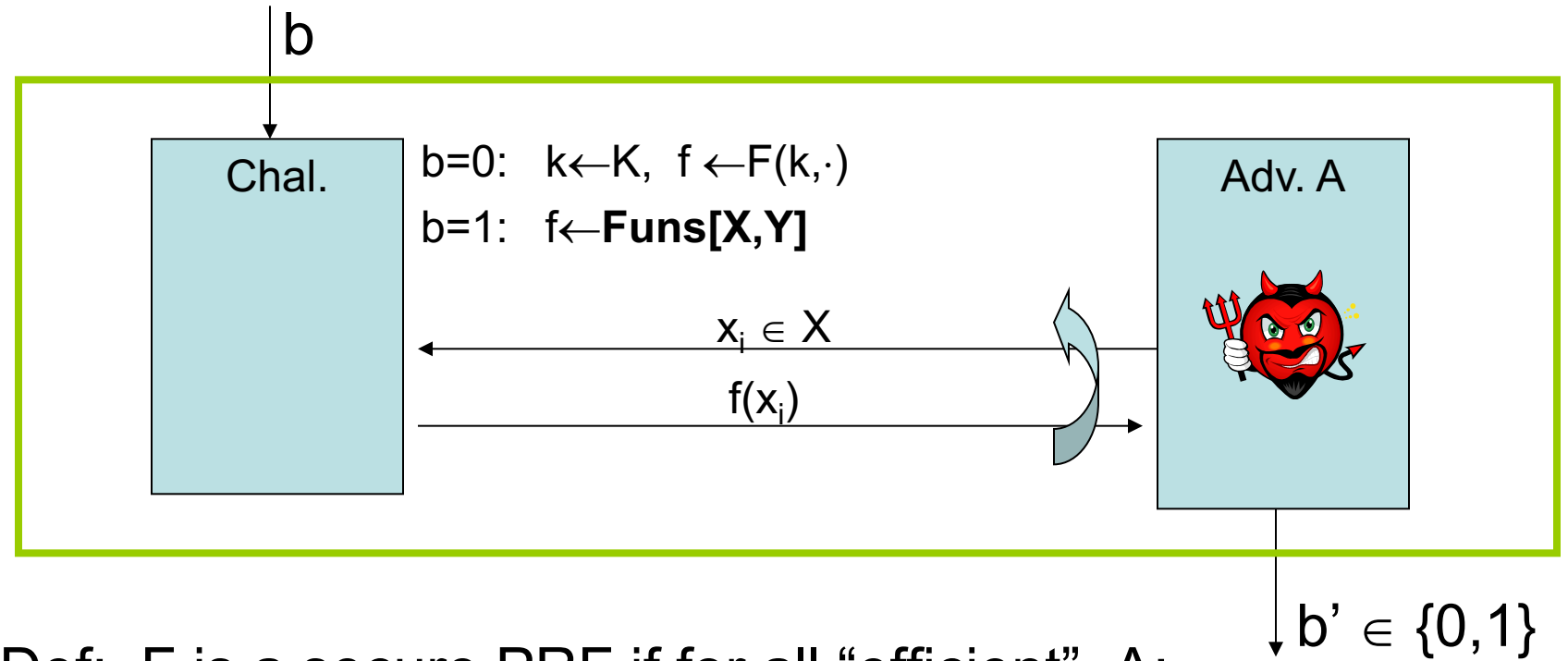
  $S_F = \{ F(k,\cdot) \text{ s.t. } k \in K \} \subseteq$ Funs[X,Y]

- Intuition: a PRF is **secure** if
  a random function in Funs[X,Y] is indistinguishable from
  a random function in S_F



Secure PRF: defintion

- For b=0,1 define experiment EXP(b) as:



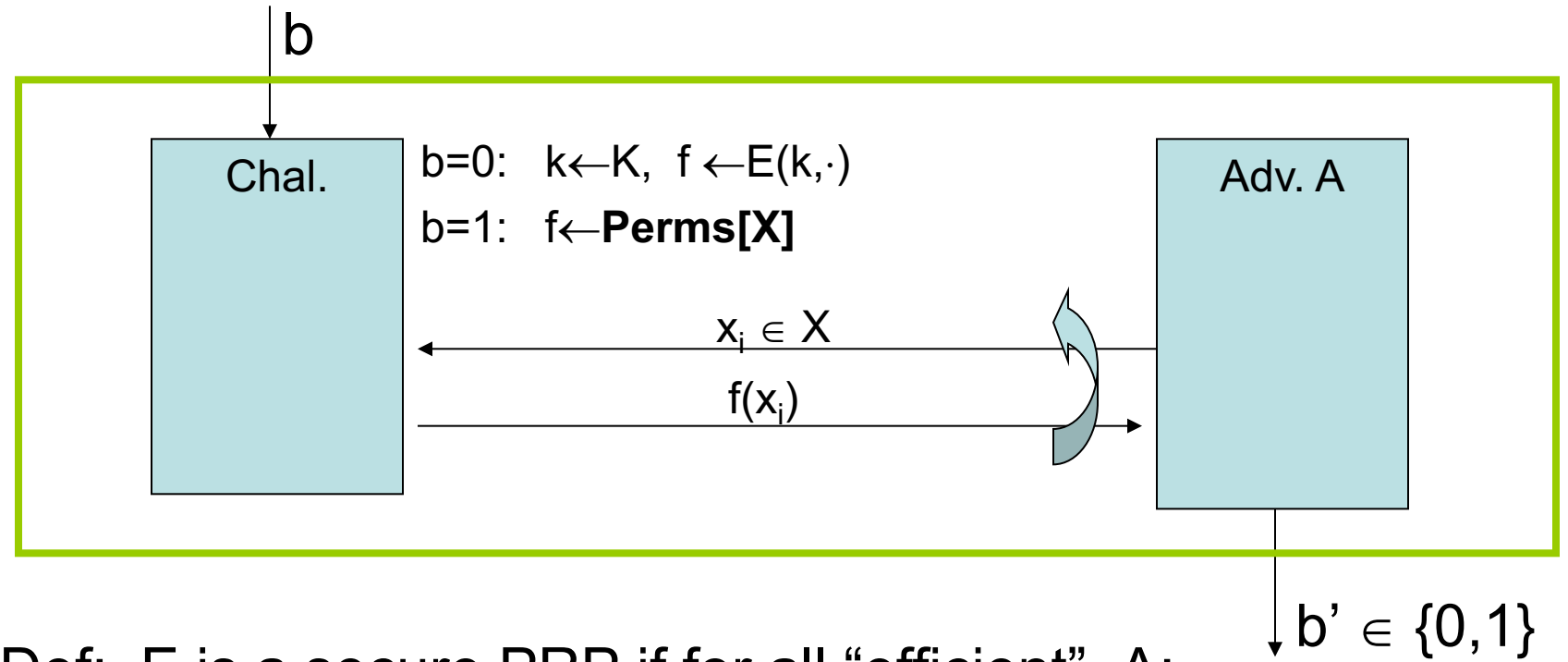
- Def: F is a secure PRF if for all "efficient" A:

$$Adv_{PRF}[A,F] = \left| Pr[EXP(0)=1] - Pr[EXP(1)=1] \right|$$

is "negligible."

Secure PRP

- For b=0,1 define experiment EXP(b) as:



- Def: E is a secure PRP if for all "efficient" A:

$$Adv_{PRP}[A,E] = \left| Pr[EXP(0)=1] - Pr[EXP(1)=1] \right|$$

is "negligible."

Example secure PRPs

- Example secure PRPs: 3DES, AES, …

  AES_{256}: $K \times X \rightarrow X$ where $X = \{0,1\}^{128}$

  $K = \{0,1\}^{256}$

- AES_{256} PRP Assumption (example) :

  All explicit 2^{80}–time algs A have PRP Adv[A, **AES_{256}**] < 2^{-40}

PRF Switching Lemma

Any secure PRP is also a secure PRF.

Lemma: Let E be a PRP over (K,X)

Then for any q-query adversary A:

$$\left| \mathrm{Adv}_{\mathrm{PRF}}[A,E] - \mathrm{Adv}_{\mathrm{PRP}}[A,E] \right| < q^2 / 2|X|$$

$\Rightarrow$ Suppose |X| is large so that $q^2 / 2|X|$ is "negligible"

Then $\mathrm{Adv}_{\mathrm{PRP}}[A,E]$ "negligible" $\Rightarrow$ $\mathrm{Adv}_{\mathrm{PRF}}[A,E]$ "negligible"

Using PRPs and PRFs

- Goal: build "secure" encryption from a PRP.

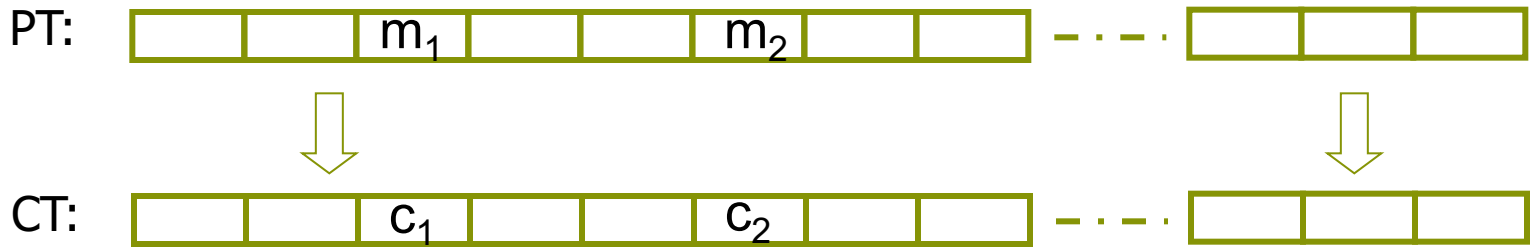
- Security is always defined using two parameters:

  1. What "**power**" does adversary have?
     examples:
     - Adv sees only one ciphertext (one-time key)
     - Adv sees many PT/CT pairs (many-time key, CPA)

  2. What "**goal**" is adversary trying to achieve?
     examples:
     - Fully decrypt a challenge ciphertext.
     - Learn info about PT from CT (semantic security)

Incorrect use of a PRP

Electronic Code Book (ECB):



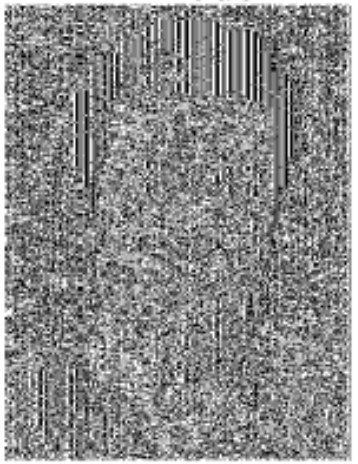
Problem:

– if $m_1=m_2$ then $c_1=c_2$

In pictures

An example plaintext

Encrypted with AES in ECB mode



(courtesy B. Preneel)