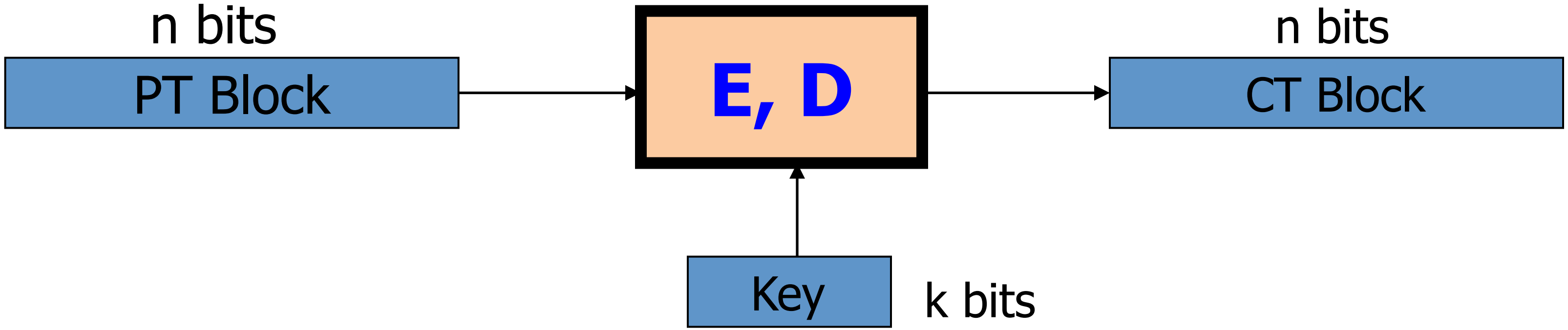
Using block ciphers

Review: PRPs and PRFs

Block ciphers: crypto work horse



Canonical examples:

1. 3DES: n= 64 bits, k = 168 bits
2. AES: n=128 bits, k = 128, 192, 256 bits

Abstractly: PRPs and PRFs

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

$$F: K \times X \longrightarrow Y$$

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

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

$$E: K \times X \longrightarrow X$$

such that:

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

Secure PRFs

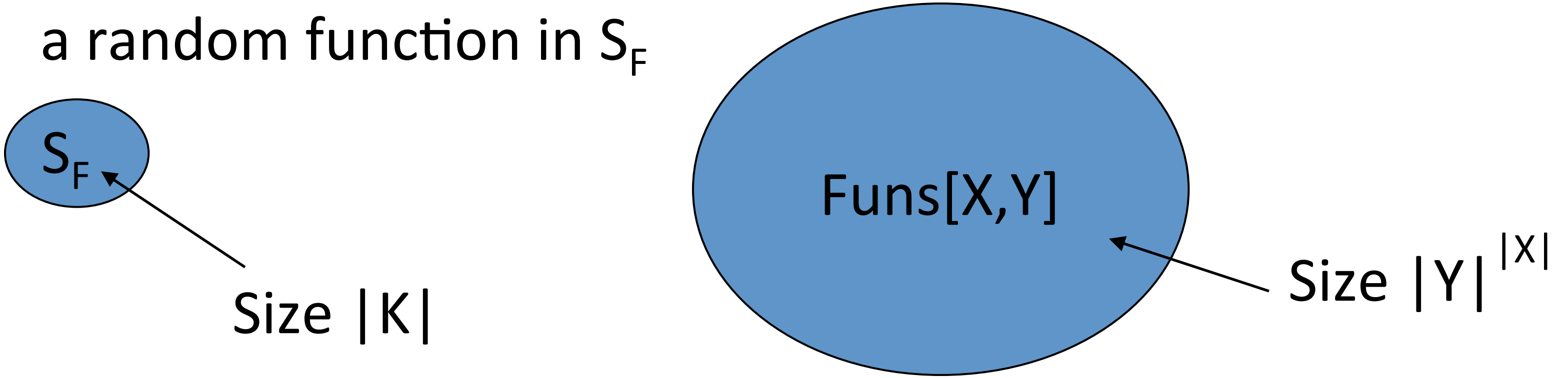
- Let $F: K \times X \longrightarrow Y$ be a PRF

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

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

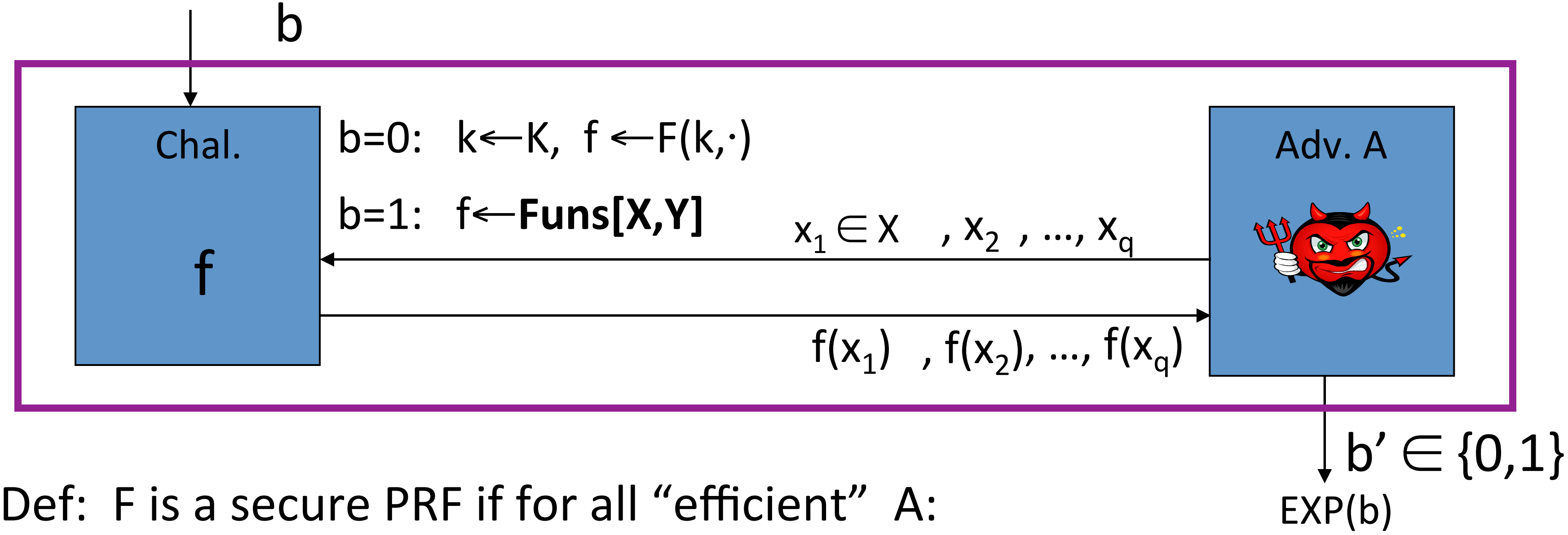
- Intuition: a PRF is **secure** if

  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:



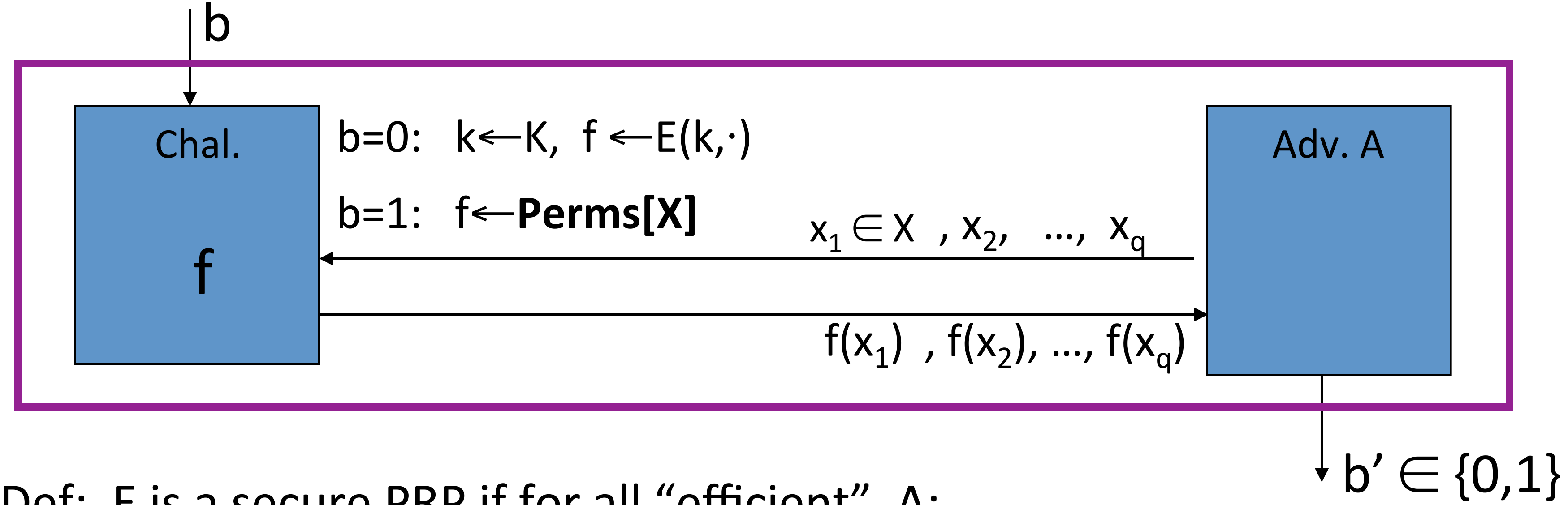
- Def: F is a secure PRF if for all "efficient" A:

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

is "negligible."

Secure PRP (secure block cipher)

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



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

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

is "negligible."

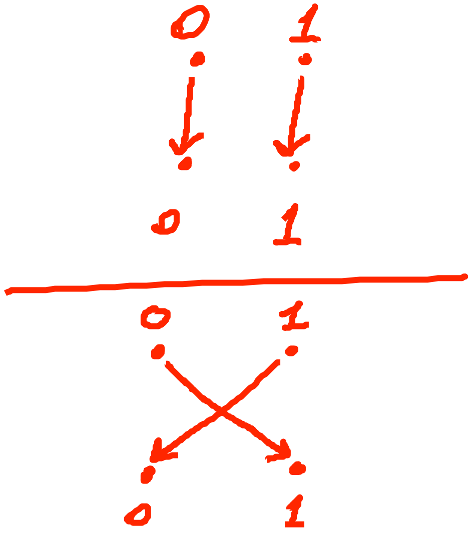
Let X = {0,1}. Perms[X] contains two functions

Consider the following PRP:

key space K={0,1}, input space X = {0,1},

PRP defined as:

$$E(k,x) = x \oplus k$$



Is this a secure PRP?

- ○ Yes
- ○ No
- ○ It depends
- ○

Example secure PRPs

- PRPs believed to be secure: 3DES, AES, …

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

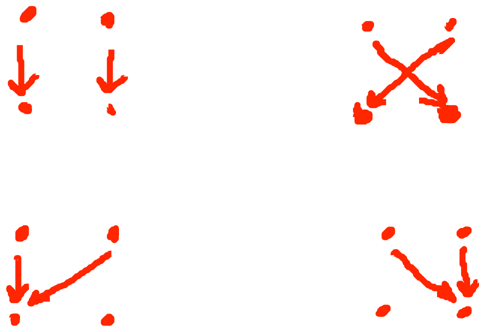
- An example concrete assumption about AES:

  All 2^{80}–time algs. A have $\mathrm{Adv}_{\mathrm{PRP}}[A, \mathbf{AES}] < 2^{-40}$

Consider the 1-bit PRP from the previous question: $E(k,x) = x \oplus k$

Is it a secure PRF?

Note that Funs[X,X] contains four functions



- ○ Yes
- ○ No
- ○ It depends
- ○

Attacker A:

(1) query $f(\cdot)$ at $x=0$ and $x=1$

(2) if $f(0) = f(1)$ output "1", else "0"

$\text{Adv}_{\text{PRF}}[A,E] = |0-½| = ½$

PRF Switching Lemma

Any secure PRP is also a secure PRF, if |X| is sufficiently large.

<u>Lemma</u>: Let E be a PRP over (K,X)

Then for any q-query adversary A:

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

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

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

Final note

- Suggestion:
  - don’t thing about the inner-workings of AES and 3DES.

- We assume both are secure PRPs and will see how to use them

End of Segment