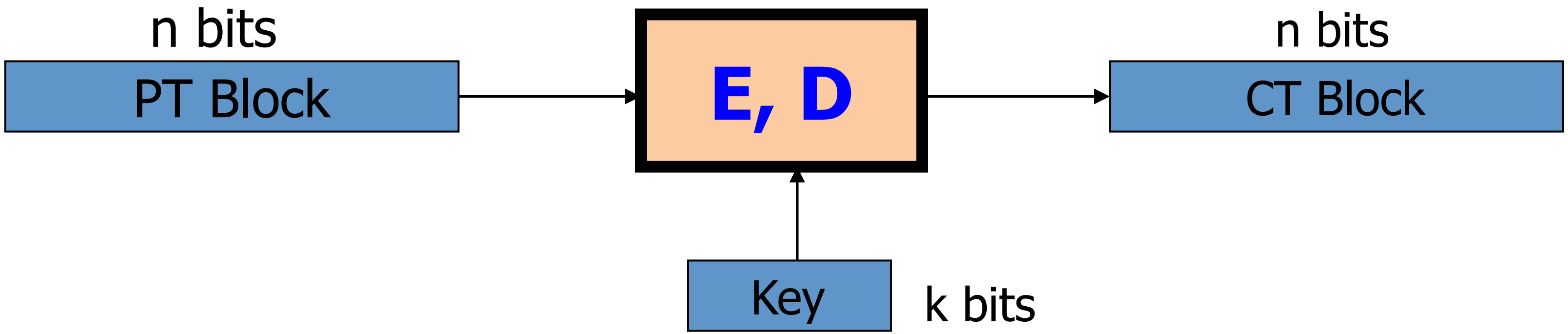
Block ciphers

What is a block cipher?

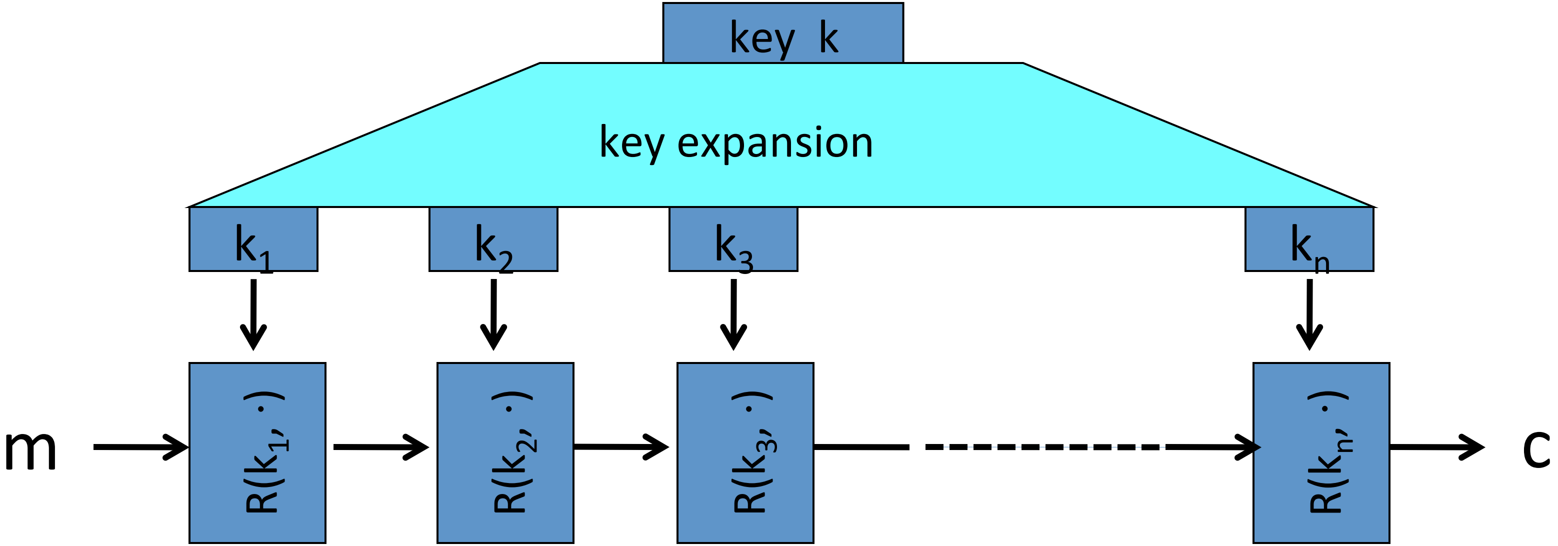
Block ciphers: crypto work horse



Canonical examples:

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

Block Ciphers Built by Iteration



R(k,m) is called a round function

for 3DES (n=48), for AES-128 (n=10)

Performance:

Crypto++ 5.6.0 [Wei Dai]

AMD Opteron, 2.2 GHz (Linux)

	Cipher	Block/key size	Speed (MB/sec)
stream	RC4		126
	Salsa20/12		643
	Sosemanuk		727
block	3DES	64/168	13
	AES-128	128/128	109

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

Running example

- Example PRPs: 3DES, AES, …

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

  3DES: $K \times X \longrightarrow X$ 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.

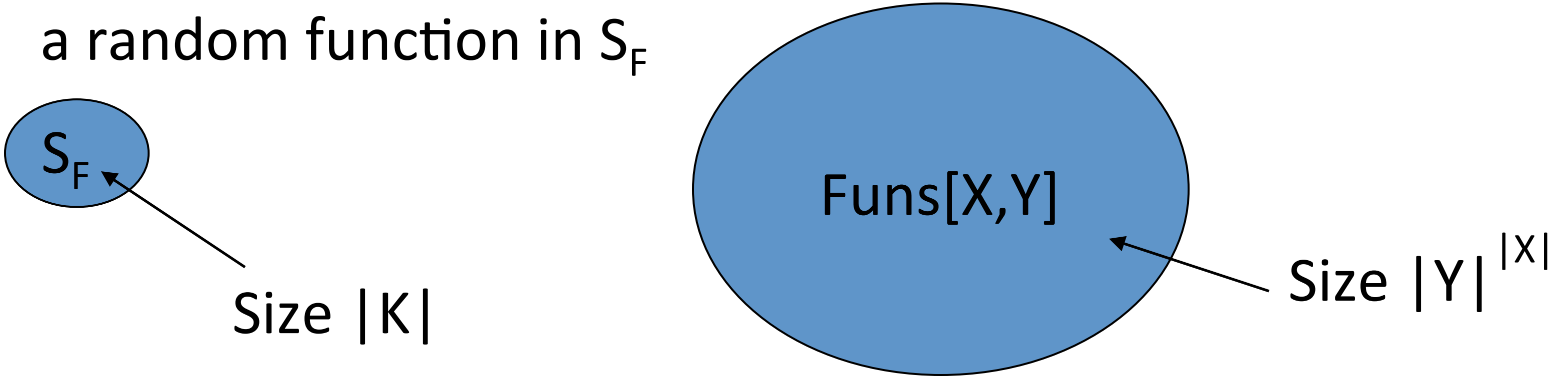
Secure PRFs

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

$$\begin{cases} \text{Funs}[X,Y]: \quad \text{the set of } \underline{\textbf{all}} \text{ functions from } X \text{ to } Y \\ S_F = \{\ F(k,\cdot)\ \text{ s.t. } k \in K\ \} \quad \subseteq \quad \text{Funs}[X,Y] \end{cases}$$

- <u>Intuition</u>: a PRF is **secure** if

  a random function in Funs[X,Y] is indistinguishable from
  a random function in S_F



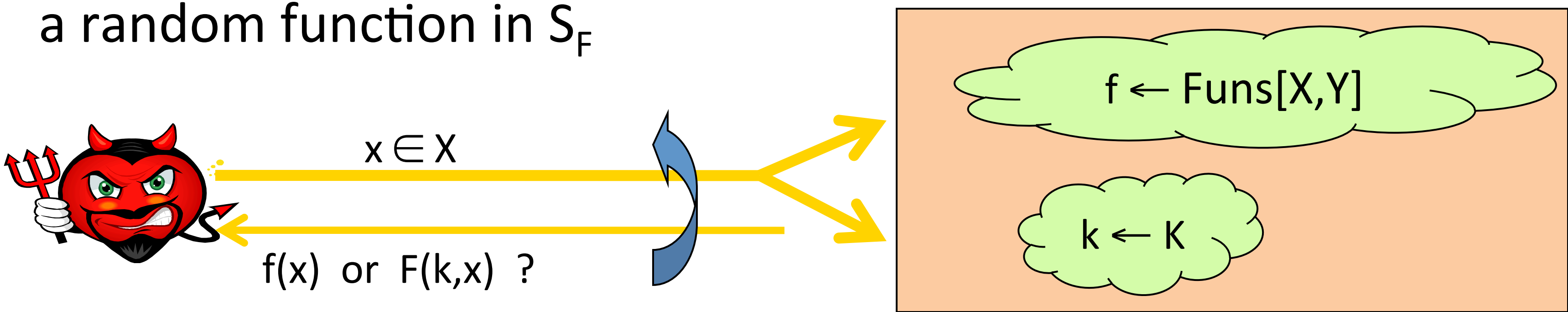
Secure PRFs

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

$$\begin{cases} \text{Funs}[X,Y]: & \text{the set of } \underline{\textbf{all}} \text{ functions from } X \text{ to } Y \\ S_F = \{\ F(k,\cdot)\ \text{ s.t. } k \in K\ \} & \subseteq \quad \text{Funs}[X,Y] \end{cases}$$

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

???



Secure PRPs (secure block cipher)

- Let $E: K \times X \rightarrow Y$ be a PRP

Perms[X]: the set of all **<u>one-to-one</u>** functions from X to Y

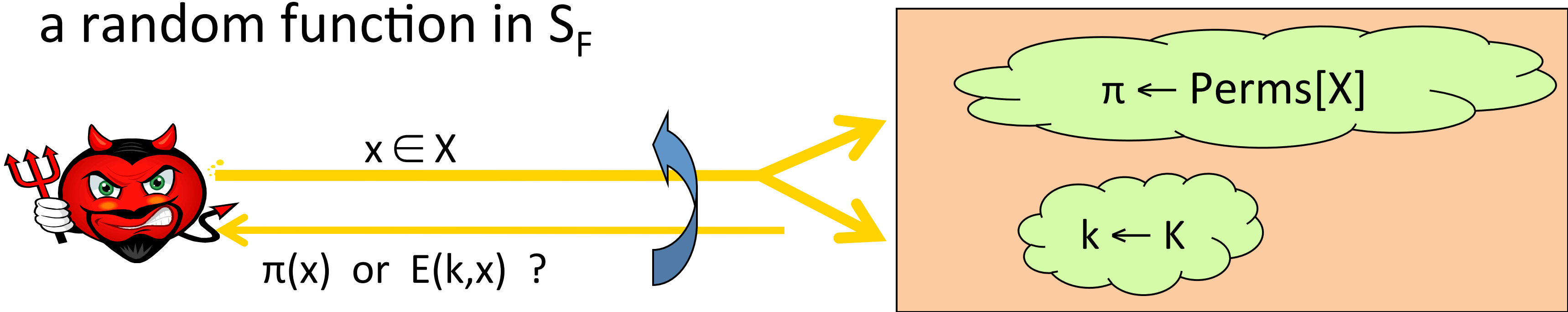
$S_F = \{ E(k,\cdot) \text{ s.t. } k \in K \} \subseteq \text{Perms}[X,Y]$

- <u>Intuition</u>: a PRP is **secure** if

  a random function in Perms[X] is indistinguishable from

  a random function in S_F

???



Let $F: K \times X \longrightarrow \{0,1\}^{128}$ be a secure PRF.

Is the following G a secure PRF?

$$G(k, x) = \begin{cases} 0^{128} & \text{if } x=0 \\ F(k,x) & \text{otherwise} \end{cases}$$

- ○ No, it is easy to distinguish G from a random function
- ○ Yes, an attack on G would also break F
- ○ It depends on F

An easy application: PRF $\Rightarrow$ PRG

Let $F: K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a secure PRF.

Then the following $G: K \longrightarrow \{0,1\}^{nt}$ is a secure PRG:

$$\mathbf{G(k) = F(k,0) \,\|\, F(k,1) \,\|\, \cdots \,\|\, F(k,t)}$$

Key property: parallelizable

Security from PRF property: $F(k, \cdot)$ indist. from random function $f(\cdot)$

End of Segment