Recall Shannon's perfect secrecy

Let (E,D) be a cipher over (K,M,C)

(E,D) has perfect secrecy if $\forall\, m_0, m_1 \in M \quad (\ |m_0| = |m_1| \ )$

$$\{ E(k,m_0) \} \quad = \quad \{ E(k,m_1) \} \qquad \text{where} \quad k \leftarrow K$$

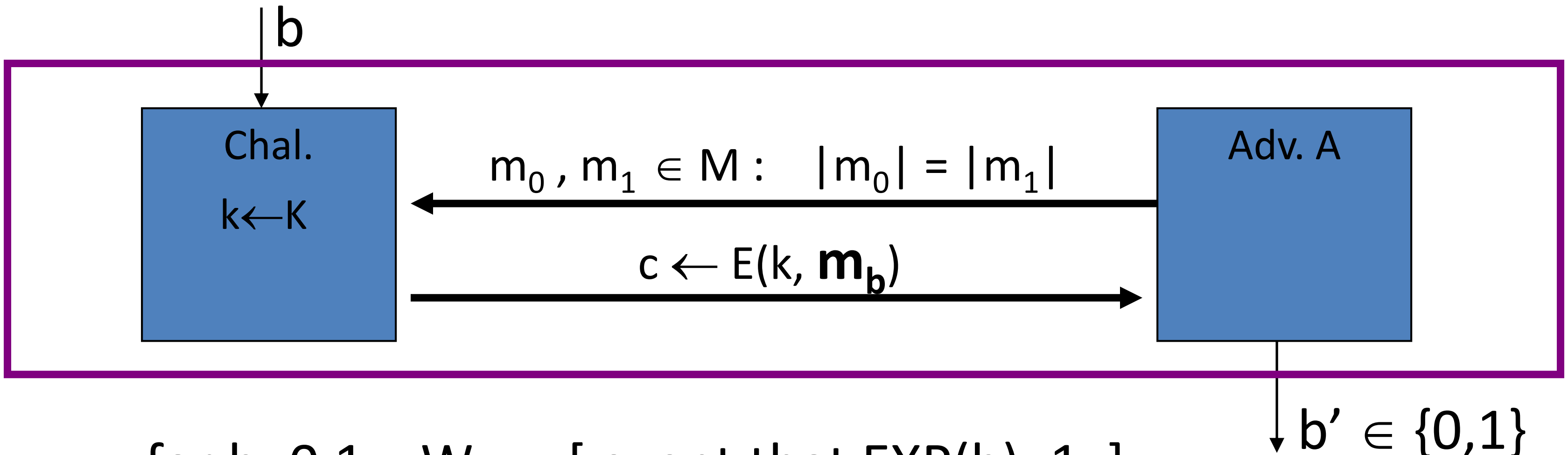
(E,D) has semantic secrecy if $\forall\, m_0, m_1 \in M \quad (\ |m_0| = |m_1| \ )$

$$\{ E(k,m_0) \} \ \approx_p \ \{ E(k,m_1) \} \qquad \text{where} \quad k \leftarrow K$$

... but also need adversary to exhibit $m_0, m_1 \in M$ explicitly

Semantic Security (one-time key)

For $b=0,1$ define experiments EXP(0) and EXP(1) as:



for $b=0,1$: W_b := [event that EXP(b)=1]

$$Adv_{SS}[A,E] := \left| \Pr[W_0] - \Pr[W_1] \right| \in [0,1]$$

Semantic Security (one-time key)

Def: $\mathbb{E}$ is **semantically secure** if for all efficient A

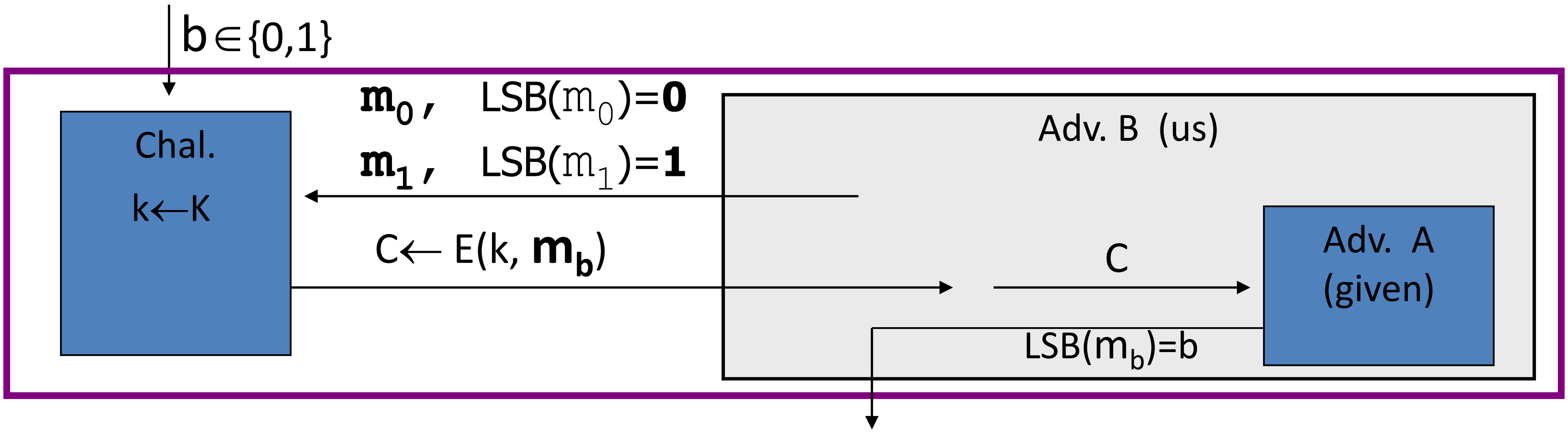
$\mathrm{Adv}_{SS}[A,\mathbb{E}]$ is negligible.

$\Rightarrow$ for all explicit $m_0, m_1 \in M$: $\{ E(k,m_0) \} \approx_p \{ E(k,m_1) \}$

Examples

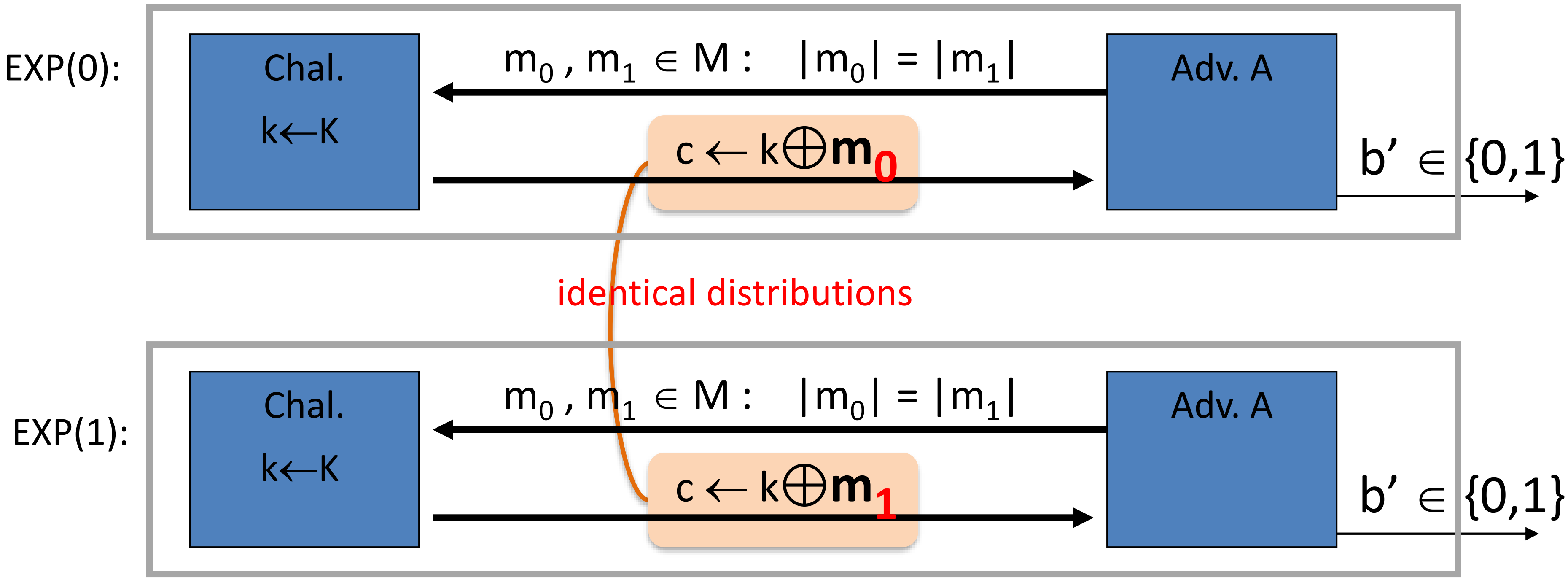
Suppose efficient A can always deduce LSB of PT from CT.

$\Rightarrow \quad \mathbb{E} = (E,D)$ is not semantically secure.



Then $\text{Adv}_{SS}[B, \mathbb{E}] = \left| \Pr[\ \mathbf{EXP(0)}=1\ ] - \Pr[\ \mathbf{EXP(1)}=1\ ] \right| =$

OPT is semantically secure



For **all** A: $\quad \text{Adv}_{SS}[A,OTP] = \Big| \Pr[\, \mathbf{A(k \oplus m_0)}=1 \,] - \Pr[\, \mathbf{A(k \oplus m_1)}=1 \,] \Big|$

Quantum Cryptography

Photo shows the U.S. journal Science with a cover story about a major technical breakthrough towards quantum communication over great distances by Chinese scientists.

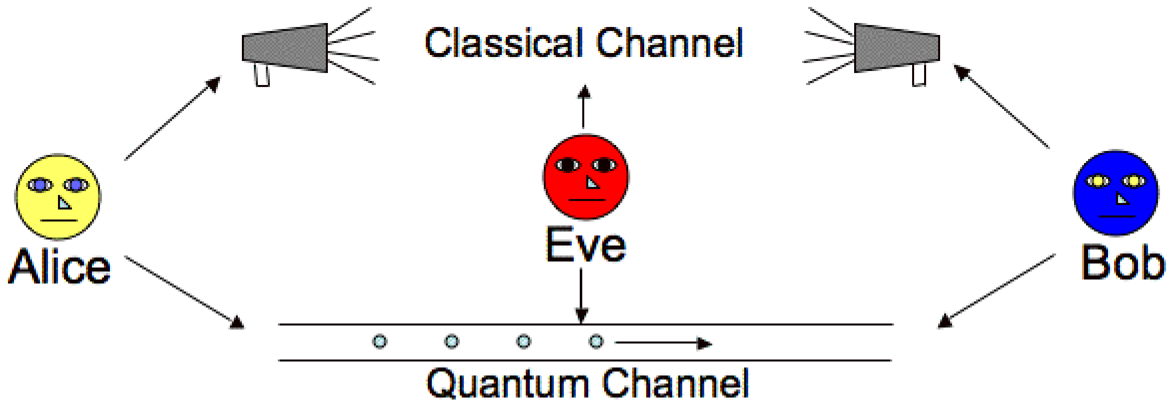
Quantum Cryptography

Quantum Cryptography = Quantum Key Distribution + One-Time Pad

↓

A secure way of establishing secret keys between two parties

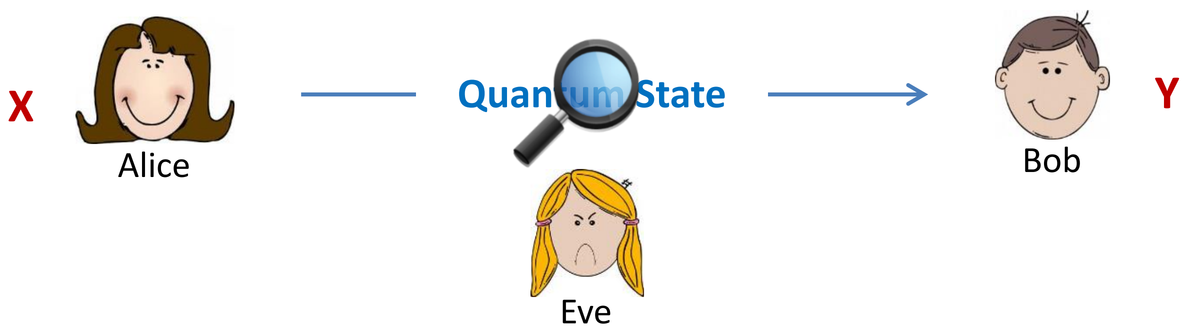
Quantum Key Distribution (QKD)



The basic model for QKD protocols involves two parties, referred to as Alice and Bob, wishing to exchange a key both with access to a classical public communication channel and a quantum communication channel. This is shown in the figure above. An eavesdropper, called Eve, is assumed to have access to both channels and no assumptions are made about the resources at her disposal.

Quantum Key Distribution (QKD)

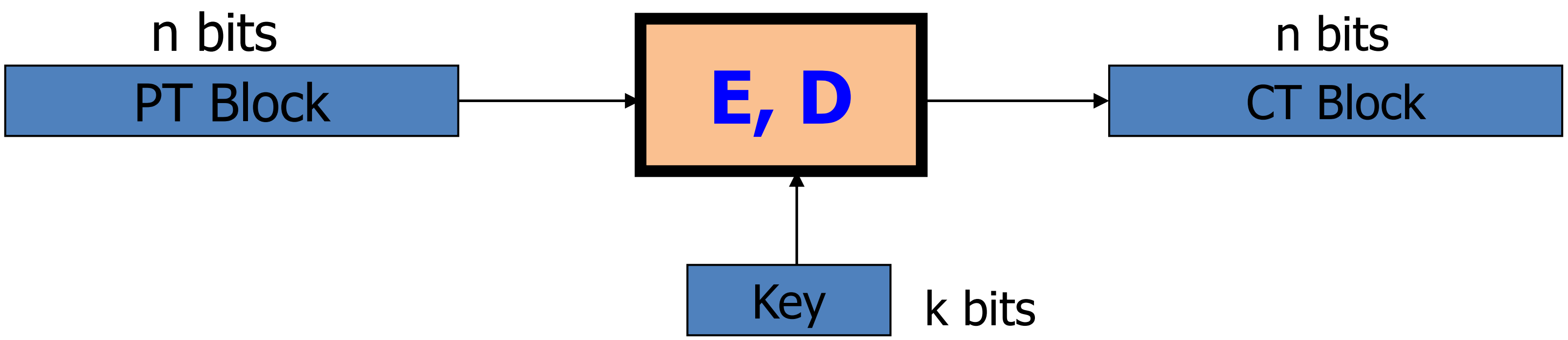
One principle of quantum mechanics, the no cloning theorem, intuitively follows from Heisenberg's Uncertainty Principle. The no cloning theorem states that it is impossible to create identical copies of an arbitrary unknown quantum state



Measurement changes quantum states

Lecture 4.3: What is Block Cipher?

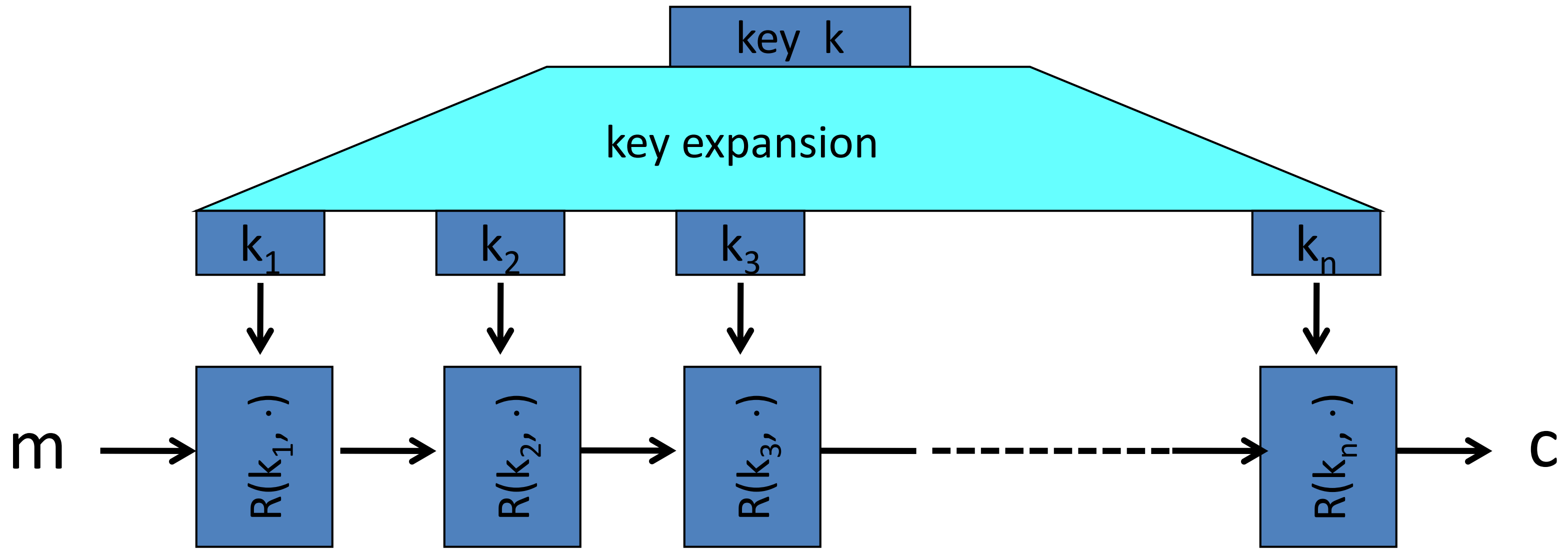
Block Ciphers: Crypto Work Horse



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)

Abstractly: 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" <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,x)

Running Example

Example PRPs: 3DES, AES, …

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

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.

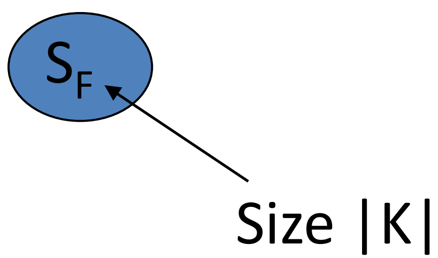
Secure PRFs

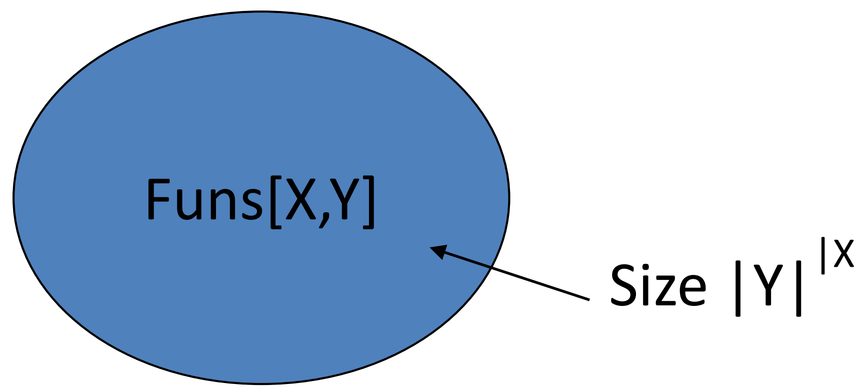
Let $F: K \times X \to Y$ be a PRF

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

<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

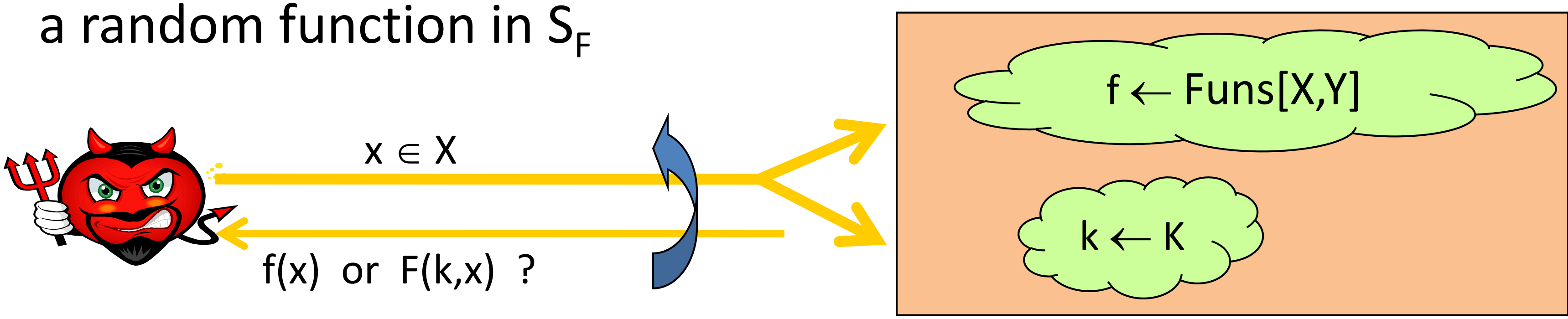
Let $F: K \times X \rightarrow Y$ be a PRF

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

<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 PRPs (secure block cipher)

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

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

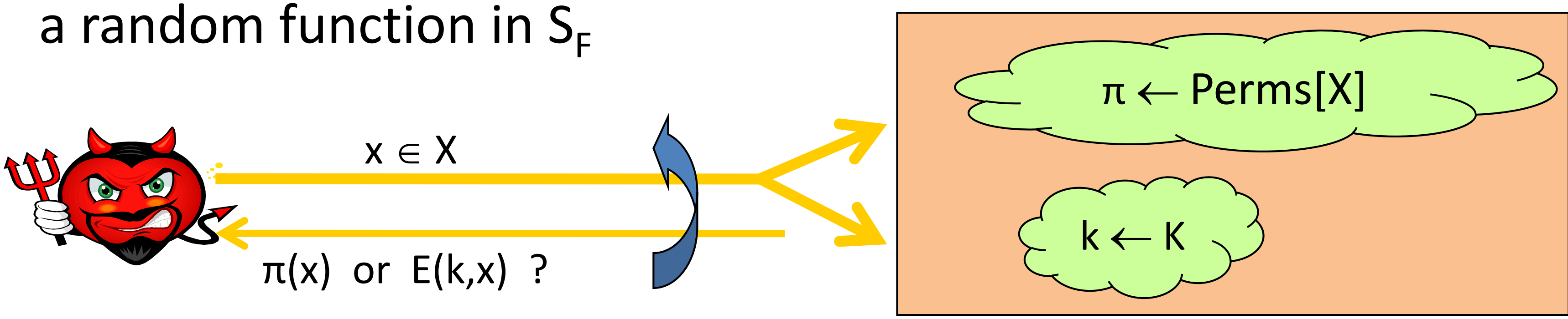
$S_F = \{ E(k,\cdot) \text{ s.t. } k \in K \} \subseteq$ Perms[X,Y]

Intuition: a PRP is **secure** if

a random function in Perms[X] is indistinguishable from

a random function in S_F

???



Question?

Let $F: K \times X \rightarrow \{0,1\}^{128}$ 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

The Data Encryption Standard (DES)

Early 1970s: Horst Feistel designs Lucifer at IBM

key-len = 128 bits ; block-len = 128 bits

1973: NBS asks for block cipher proposals.

IBM submits variant of Lucifer.

1976: NBS adopts DES as a federal standard

key-len = 56 bits ; block-len = 64 bits

1997: DES broken by exhaustive search

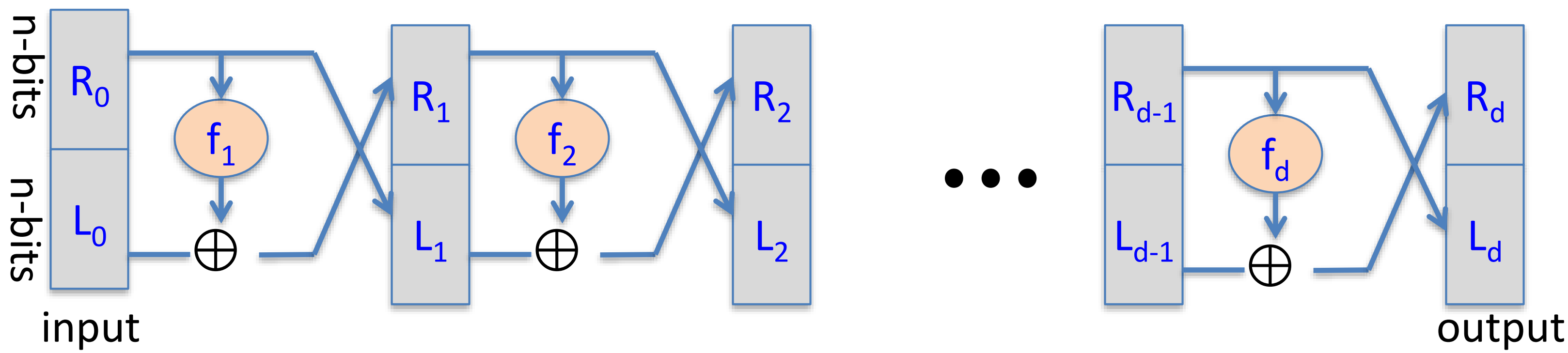
2000: NIST adopts Rijndael as AES to replace DES

Widely deployed in banking (ACH) and commerce

DES: Core Idea – Feistel Network

Given functions $f_1, \ldots, f_d: \{0,1\}^n \longrightarrow \{0,1\}^n$

Goal: build invertible function $F: \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$

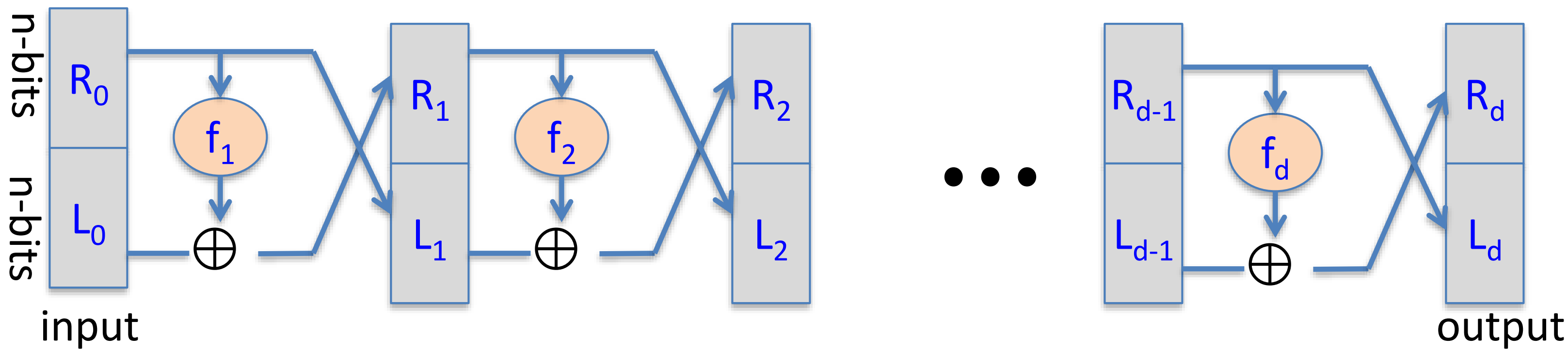


In symbols:

$$R_i = f(R_{i-1}) \oplus L_{i-1}$$

$$L_i = R_{i-1}$$

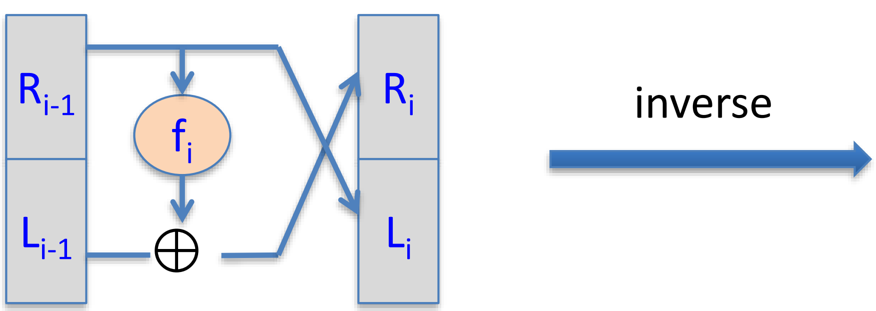
DES: Core Idea – Feistel Network



Claim: for all $f_1, \ldots, f_d : \{0,1\}^n \longrightarrow \{0,1\}^n$

Feistel network $F: \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$ is invertible

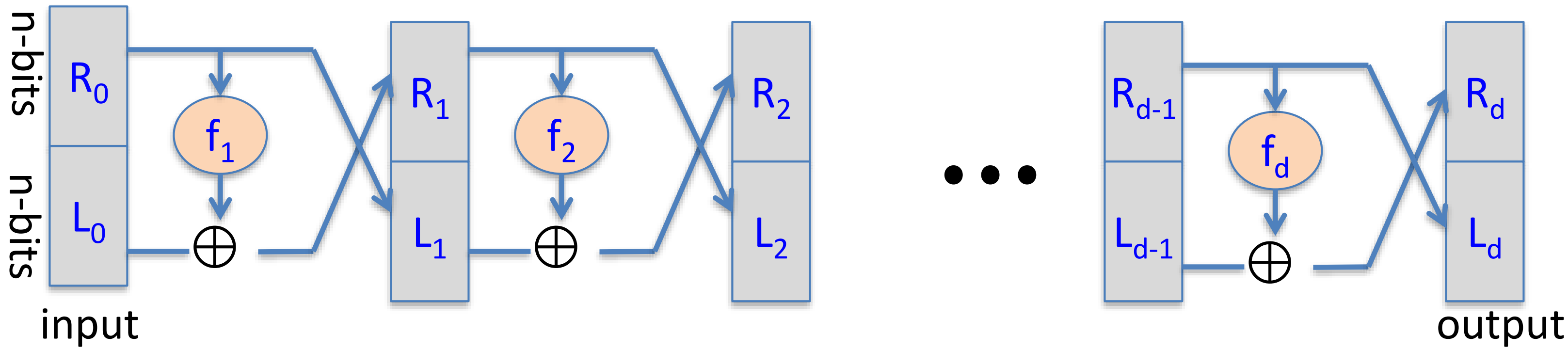
Proof: construct inverse



$R_{i-1} = L_i$

$L_{i-1} =$

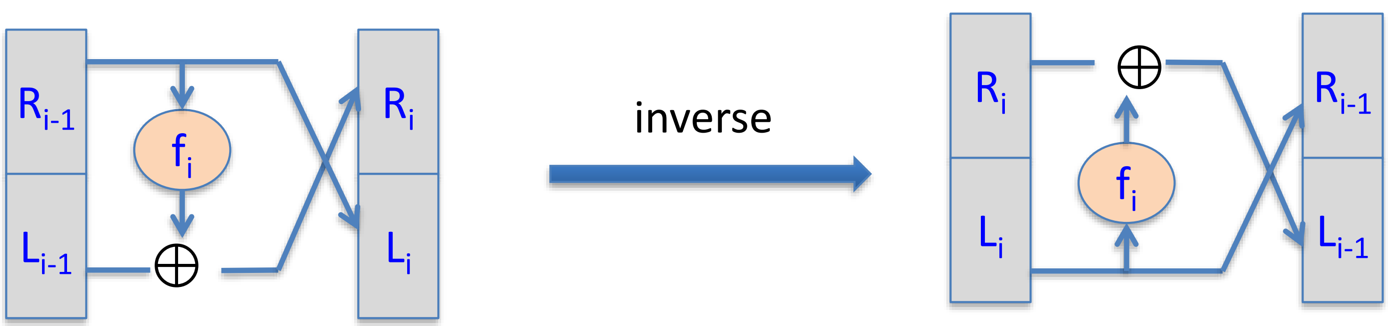
DES: Core Idea – Feistel Network



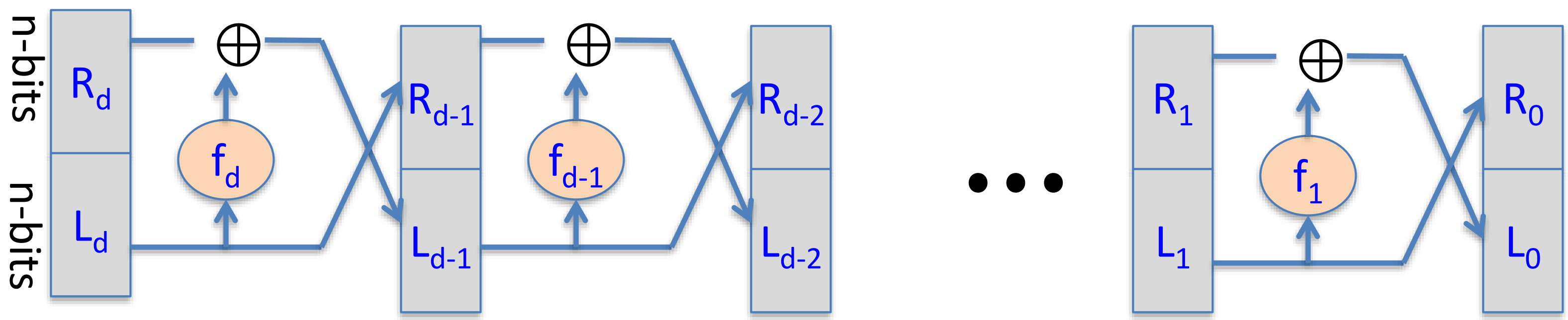
Claim: for all $f_1, \ldots, f_d$: $\{0,1\}^n \longrightarrow \{0,1\}^n$

Feistel network $F: \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$ is invertible

Proof: construct inverse



Decryption Circuit



Inversion is basically the same circuit,
with $f_1, \ldots, f_d$ applied in reverse order

General method for building invertible functions (block ciphers) from arbitrary functions.

Used in many block ciphers … but not AES

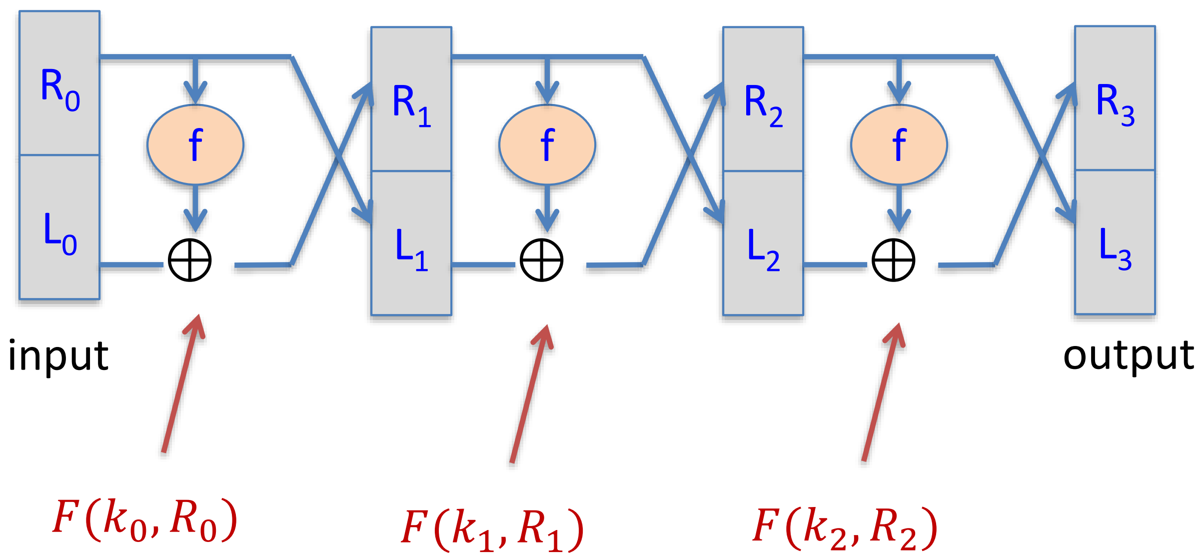
Secure PRP

"Thm:" (Luby-Rackoff '85):

f: $K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ a secure PRF

$\Rightarrow$ 3-round Feistel F: $K^3 \times \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$ a secure PRP

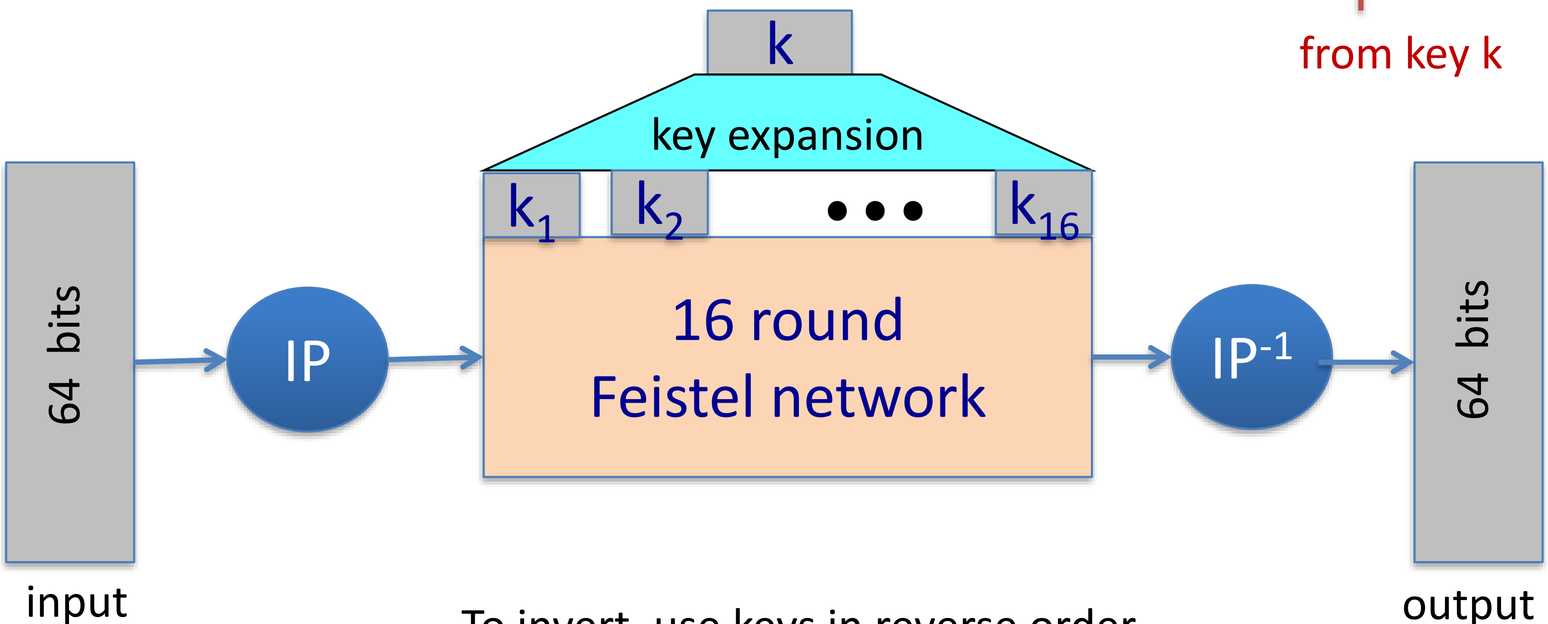
Type equation here.



DES: 16 round Feistel network

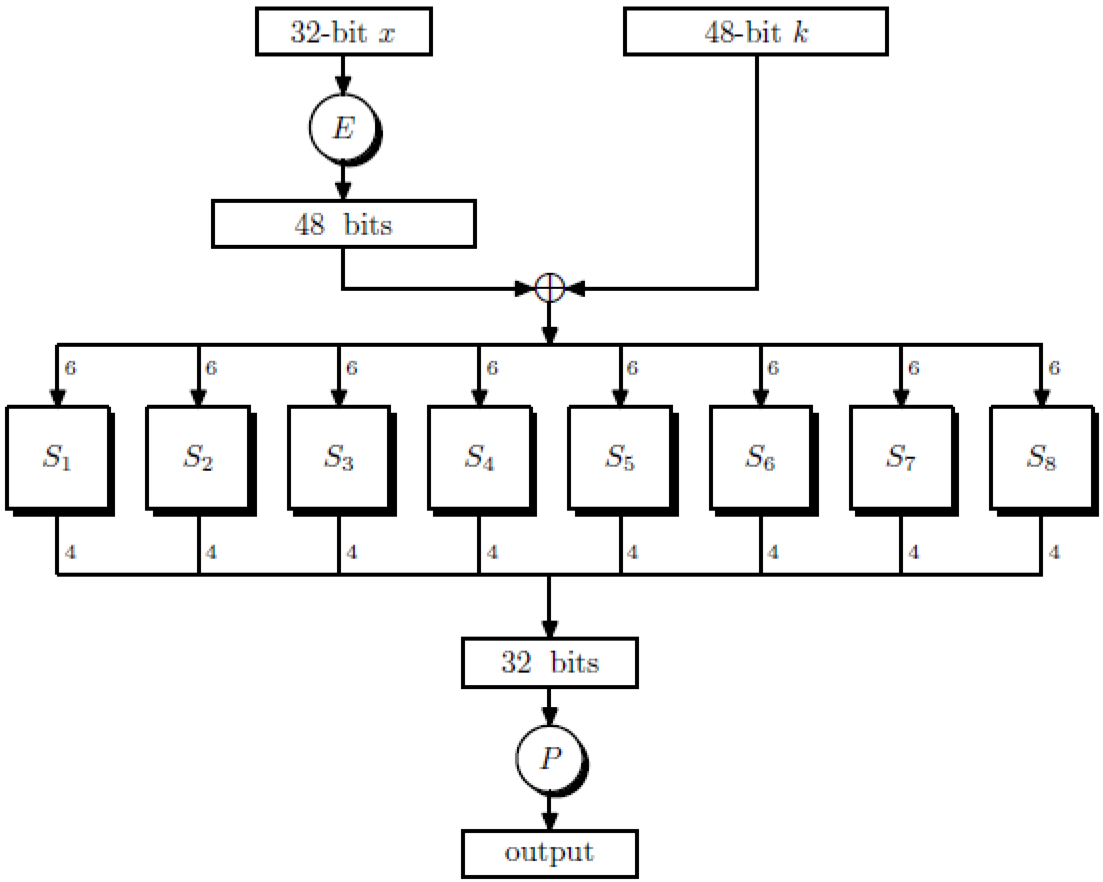
$f_1, \ldots, f_{16}: \{0,1\}^{32} \longrightarrow \{0,1\}^{32}$, $f_i(x) = \mathbf{F}(k_i, x)$

from key k



To invert, use keys in reverse order

The function $F(k_i, x)$



S-box: function $\{0,1\}^6 \longrightarrow \{0,1\}^4$, implemented as look-up table.

The S-Boxes

$$S_i: \{0,1\}^6 \longrightarrow \{0,1\}^4$$

S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

E-Box / P-Box

- Expansion/permutation

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

- Permutation

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Exhaustive Search for Block Cipher Key

Goal: given a few input output pairs $\left(m_i,\ c_i = E(k,\ m_i)\right)$ i=1,..,3
find key k.

Lemma: Suppose DES is an ***ideal cipher***

(2^{56} random invertible functions)

Then $\forall$ m, c there is at most **one** key k s.t. c = DES(k, m)

with prob. ≥ 1 – 1/256 ≈ 99.5%

Proof:

$$\Pr[\exists\, k' \neq k, \qquad \mathrm{DES}(k,m) = DES(k',m)]$$

$$\leq \sum_{k' \in \{0,1\}^{56}} \Pr[DES(k,m) = DES(k',m)] \leq \frac{2^{56}}{2^{64}} = 1/256$$

Exhaustive Search for Block Cipher Key

For two DES pairs $\big(m_1,\ c_1=\text{DES}(k,\ m_1)\big),\ \ \big(m_2,\ c_2=\text{DES}(k,\ m_2)\big)$

unicity prob. $\approx\ 1 - 1/2^{71}$

For AES-128: given two inp/out pairs, unicity prob. $\approx\ 1 - 1/2^{128}$

$\Rightarrow$ two input/output pairs are enough for exhaustive key search.

DES Challenge

msg = "`The unknown messages is:` XXXX … "

CT = c_1 c_2 c_3 c_4

Goal: find $k \in \{0,1\}^{56}$ s.t. $DES(k, m_i) = c_i$ for $i=1,2,3$

1997: Internet search -- **3 months**

1998: EFF machine (deep crack) -- **3 days** (250K \$)

1999: combined search -- **22 hours**

2006: COPACOBANA (120 FPGAs) **--** **7 days** (10K \$)

$\Rightarrow$ 56-bit ciphers should not be used !! (128-bit key $\Rightarrow 2^{72}$ days)

Linear Attacks

Given *many* inp/out pairs, can recover key in time less than 2^{56} .

<u>Linear cryptanalysis</u> (overview) : let c = DES(k, m)

Suppose for random k,m :

$$\Pr\Big[\ \underbrace{m[i_1]\oplus\cdots\oplus m[i_r]}_{\text{Subset of message bits}}\ \bigoplus\ c[j_j]\oplus\cdots\oplus c[j_v] = k[l_1]\oplus\cdots\oplus k[l_u]\ \Big] = ½ + \varepsilon$$

For some ε. For DES, this exists with $\varepsilon = 1/2^{21} \approx 0.0000000477$

Linear Attacks

$$\Pr\left[\ m[i_1]\oplus\cdots\oplus m[i_r]\ \bigoplus\ c[j_j]\oplus\cdots\oplus c[j_v]\ =\ k[l_1]\oplus\cdots\oplus k[l_u]\ \right] = ½ + ε$$

Thm: given $1/ε^2$ random $\big($m, c=DES(k, m)$\big)$ pairs then

$$k[l_1,\ldots,l_u]\ =\ \mathrm{MAJ}\left[\ m[i_1,\ldots,i_r]\ \bigoplus\ c[j_j,\ldots,j_v]\ \right]$$

with prob. ≥ 97.7%

⇒ with $1/ε^2$ inp/out pairs can find $k[l_1,\ldots,l_u]$ in time $≈1/ε^2$.

Lesson

A tiny bit of linearly in S_5 lead to a 2^{42} time attack.

$\Rightarrow$ don't design ciphers yourself !!

The AES Process

1997: NIST publishes request for proposal

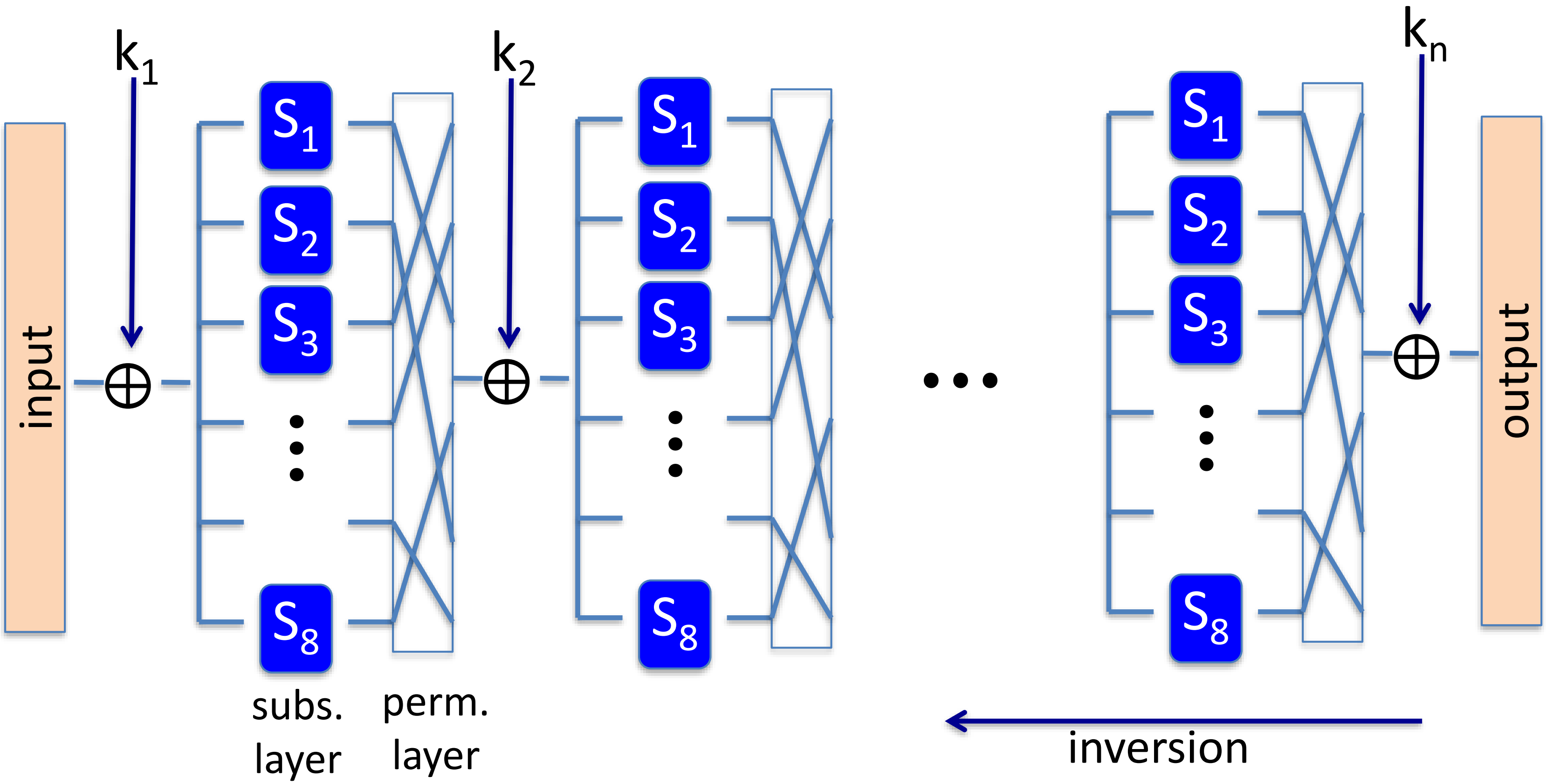
1998: 15 submissions. Five claimed attacks.

1999: NIST chooses 5 finalists

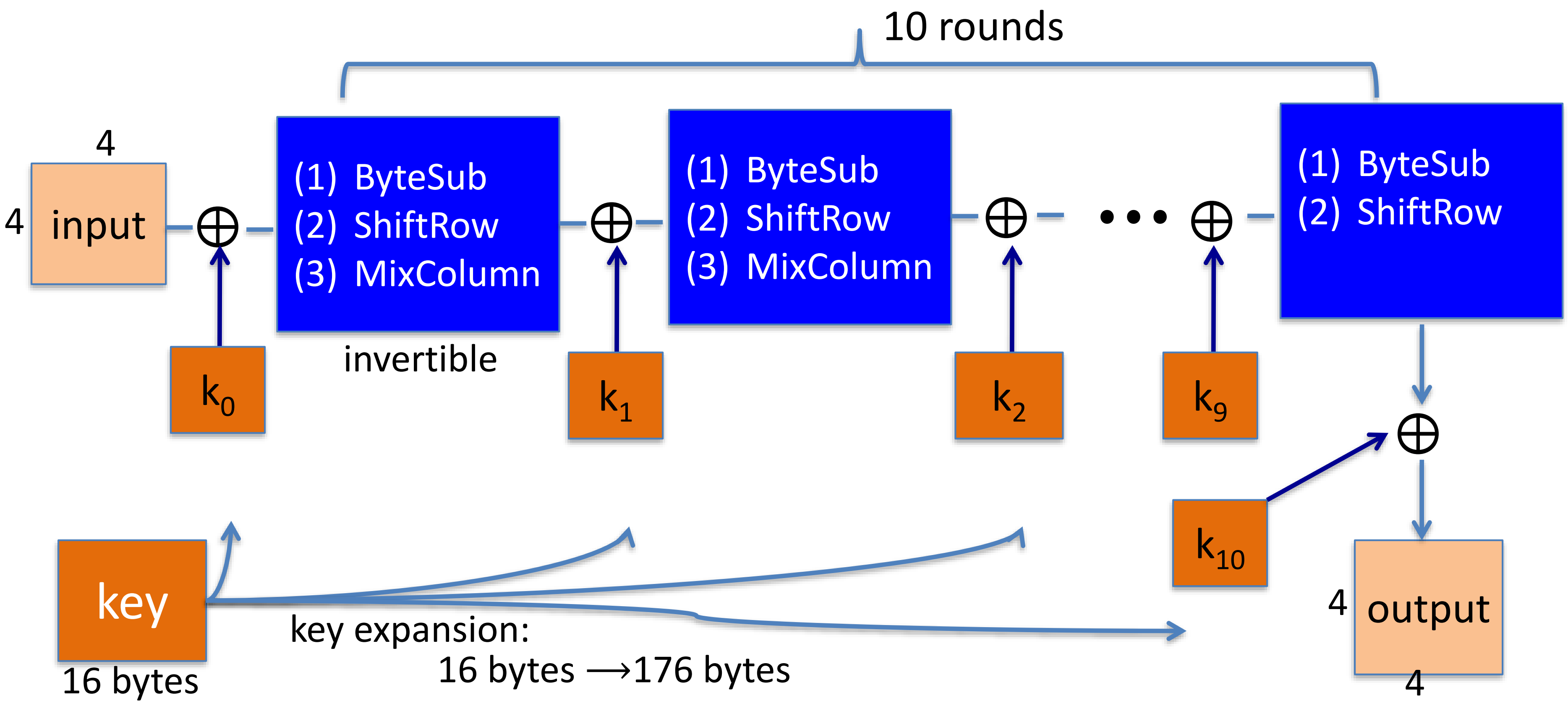
2000: NIST chooses Rijndael as AES (designed in Belgium)

Key sizes: 128, 192, 256 bits. Block size: 128 bits

AES is a Subs-Perm Network (not Feistel)



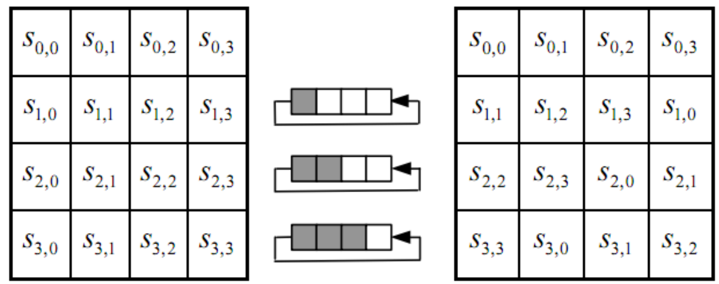
AES-128 Schematic



The Round Function

ByteSub: a 1 byte S-box. 256 byte table (easily computable)

ShiftRows:



MixColumns: