{ CSCI 6331 · 4331 | Lecture 4 }

Cryptography

Hoeteck Wee · hoeteck@gwu.edu

http://tinyurl.com/cryptogw/

Announcements

- Evaluation:

  10% In-Class/Piazza, 20% Final Presentation / Project

  30% Homework, 40% Final (Apr 25)

- Homework 2 is out

  due next Wed in class

Today

- Last week: showed how to build encryption schemes from block ciphers (PRPs)

  Q. how do we build block ciphers?

Today.

- Look at block ciphers used in practice – DES, AES

— withstood many years of public scrutiny and attempted cryptanalysis

— "design principles": Substitution-Permutation and Feistel Networks

— basic attacks

Pseudorandom Permutations (PRP) aka Block Ciphers

Pseudorandom Permutations (PRP) defined over (K, X):

$$\mathrm{E} : \mathrm{K} \times \mathrm{X} \to \mathrm{X} \quad (\text{input = output = } \mathrm{X})$$

- "efficient" algorithm to evaluate $\mathrm{E}(\mathrm{k}, \mathrm{x})$
- function $\mathrm{E}(\mathrm{k}, \cdot)$ is one-to-one
- "efficient" inversion algorithm $\mathrm{D}(\mathrm{k}, \mathrm{x})$

example. AES : $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$;

DES : $\{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$

Pseudorandom Permutations (PRP) aka Block Ciphers

Pseudorandom Permutations (PRP) defined over (K, X):

$$\mathrm{E} : \mathrm{K} \times \mathrm{X} \to \mathrm{X} \quad (\text{ input = output = } \mathrm{X} \text{ })$$

1. (challenge bit) random bit $\mathrm{b} \leftarrow \{0, 1\}$.
2. (challenge function) if $\mathrm{b} = 1$, f is truly random permutation from X to X;

   if $\mathrm{b} = 0$, f is $\mathrm{E}(\mathrm{k}, \cdot)$ for a random k
3. $\mathcal{A}$ gets $\mathrm{f}(0), \mathrm{f}(1), \mathrm{f}(2), \ldots$
4. $\mathcal{A}$ outputs b' and wins if $\mathrm{b}' = \mathrm{b}$

definition. $\mathrm{F} : \mathrm{K} \times \mathrm{X} \to \mathrm{X}$ is (t, ϵ)-secure PRP if for all adversaries $\mathcal{A}$ running in time t, winning probability bounded by $1/2 + \epsilon$

AES Assumption. AES : $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ is a $(2^{80}, 2^{-40})$-secure PRP

Basic Attack I

Brute Force Attack.

- try all possible keys k, check if f is $\mathrm{E}(\mathrm{k}, \cdot)$
- adversary $\mathcal{A}$ attacking PRP defined over (K, X):

— for every key $\mathrm{k} \in \mathrm{K}$,

check if $\mathrm{f}(0) = \mathrm{E}(\mathrm{k}, 0)$, $\mathrm{f}(1) = \mathrm{E}(\mathrm{k}, 1)$, $\mathrm{f}(2) = \mathrm{E}(\mathrm{k}, 2)$, . . .

— output 1 if such a k exists

- example: DES : $\{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$
- running time? $\approx 2^{56}$
- winning probability?

Paradigm I: Substitution-Permutation Networks

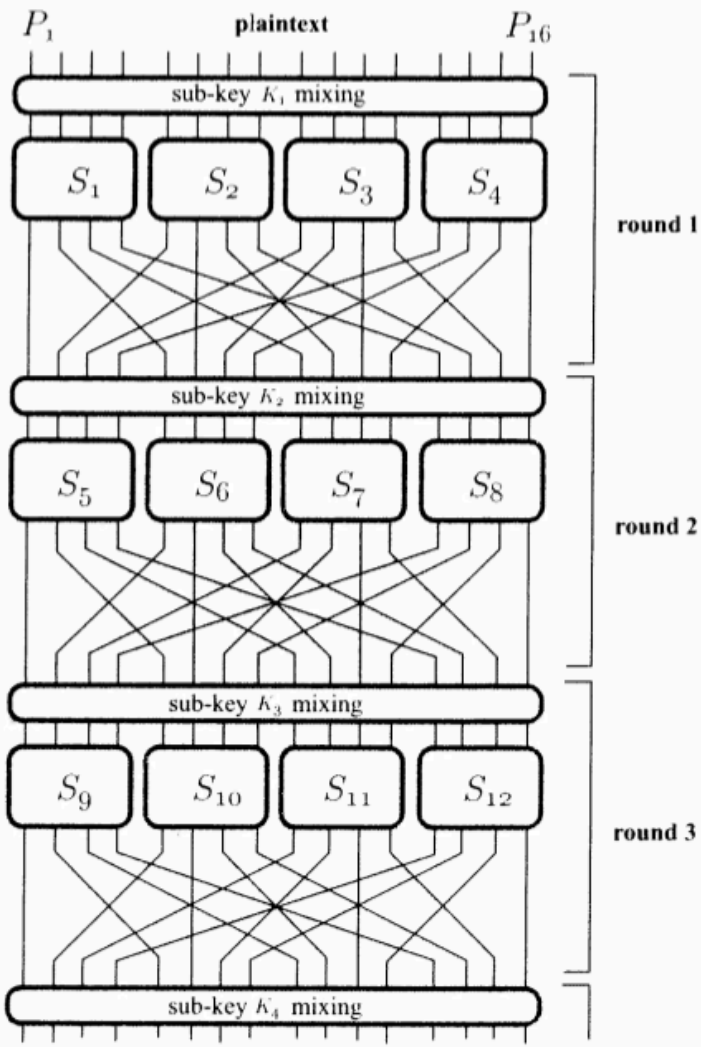


FIGURE 5.1: A substitution-permutation network.

- input/ouput $\mathrm{X} = \{0,1\}^{128}$
- break into 16 blocks of 8 bits each
- derive from key k many sub-keys $\mathrm{K}_1, \mathrm{K}_2, \ldots$
- $\mathrm{S}_1, \mathrm{S}_2, \ldots$ are fixed permutations (S-boxes)
- Principle 1.

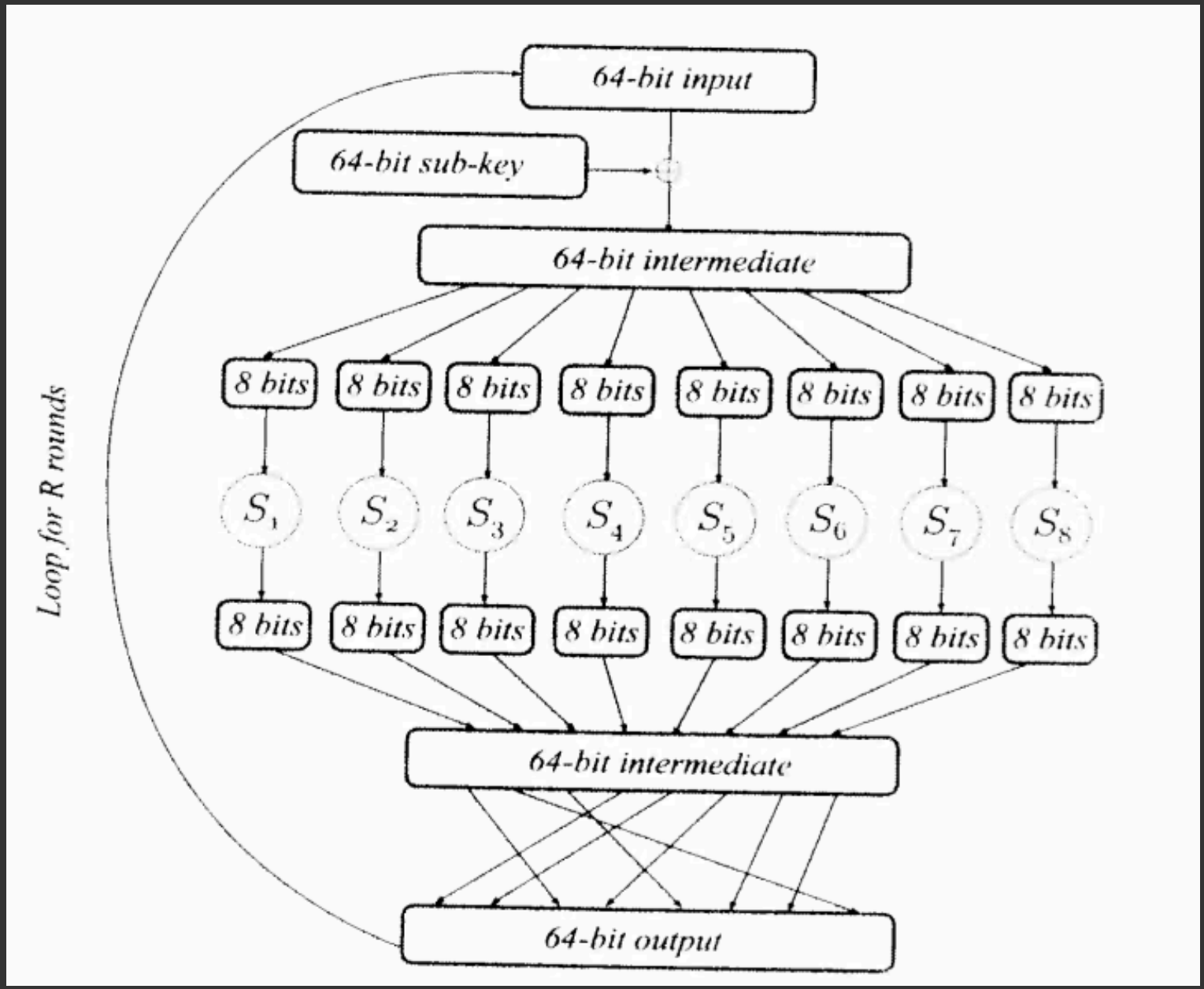
  S boxes should be invertible (why?)
- Principle 2. avalanche effect

— small changes to input $\Rightarrow$ large changes to output (why?)

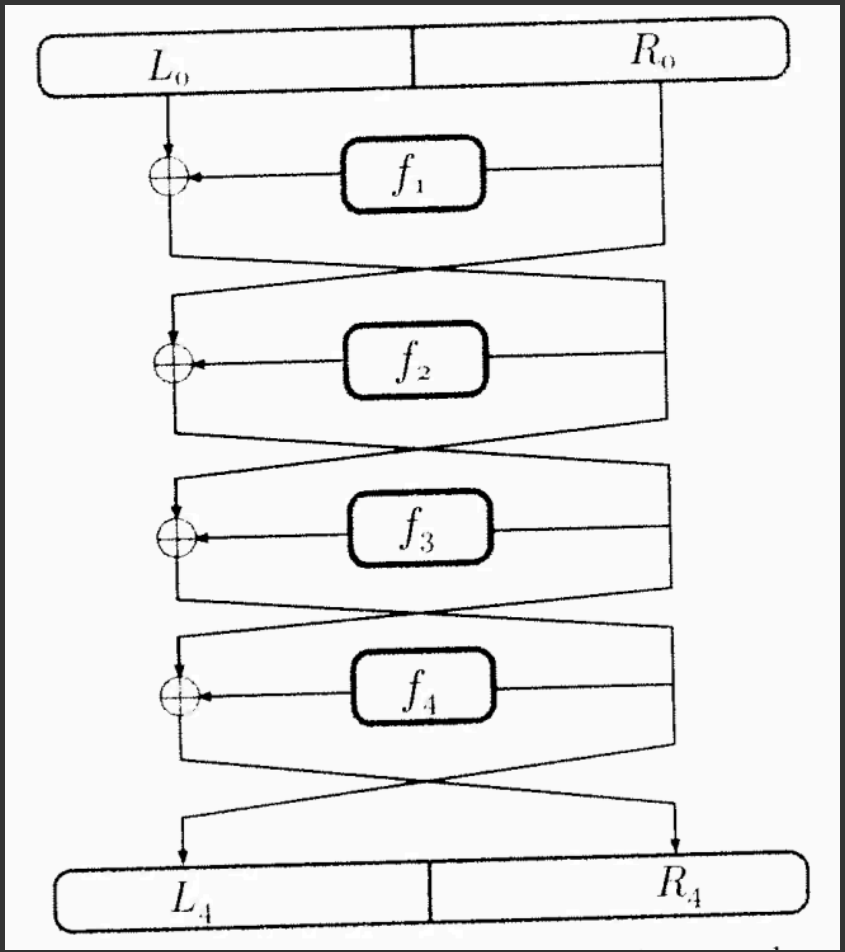
— holds for S-boxes, use many rounds

— mixing permutations: spread to different S-bxoes

Paradigm I: Substitution-Permutation Networks



Paradigm II: Feistel Networks



- eliminates invertible S-boxes
- build invertible function from non-invertible components
- derive from key $\mathrm{f}_1, \mathrm{f}_2, \ldots$
- $(\mathrm{L}_0, \mathrm{R}_0) \mapsto (\mathrm{R}_0, \mathrm{L}_0 \oplus \mathrm{f}_1(\mathrm{R}_0))$

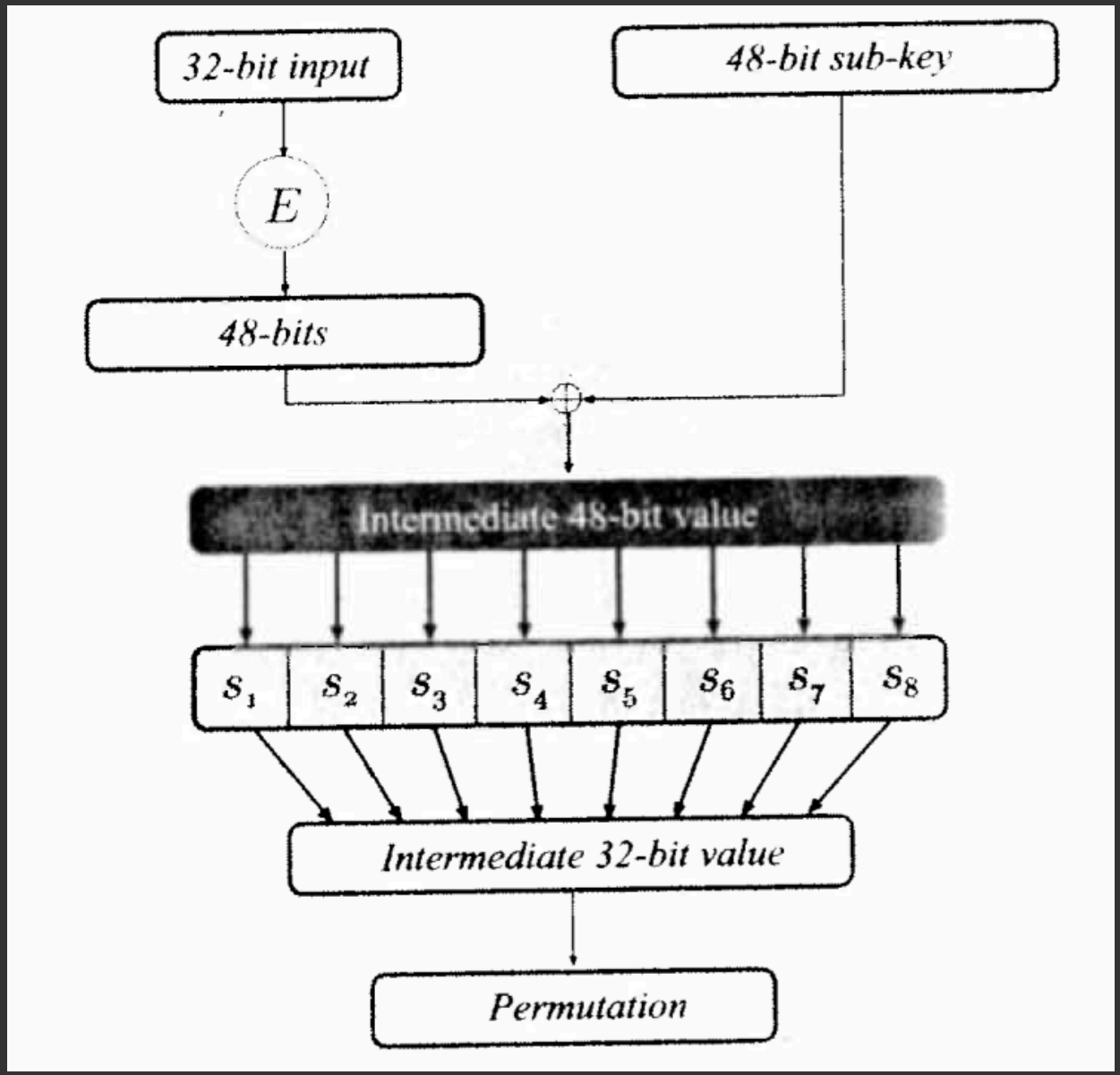
  Q. how to invert?

Case Study I: DES

DES. Data Encryption Standard; DES : $\{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$

- developed 1970s by IBM (+ NSA), adopted 1977
- 16-round Feistel network
- $\mathrm{f}_1, \ldots, \mathrm{f}_{16} : \{0,1\}^{32} \to \{0,1\}^{32}$ depends on 48-bit subkeys derived from 56-bit key
- built using a 1-round substitution-permutation network

Case Study I: DES



Case Study I: DES

DES. Data Encryption Standard; DES : $\{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$

- developed 1970s by IBM (+ NSA), adopted 1977
- 16-round Feistel network
- $f_1, \ldots, f_{16} : \{0,1\}^{32} \to \{0,1\}^{32}$ depends on 48-bit subkeys derived from 56-bit key

Attacks. Brute-force search 2^{56}

- latest challenge solved in just over 22 hours
- key length is too short for use today

Triple-DES

- Triple-DES : DES_{k_1} (DES_{k_2} (DES_{k_3} (input)))
- "meet-in-the-middle" attack $\approx 2^{112}$

Case Study II: AES

AES. Advanced Encryption Standard; AES : $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$

- selected in 2000 from 1997 NIST competition
- "winning" entry : Rijndael (by Daemen & Rijmen)
- free, standardized, efficient, and highly secure
- substitution-permutation network
- 10 rounds for 128-bit key, 12 rounds for 192-bit key, 14 rounds for 256-bit key

Message Integrity

Goal. Protect Integrity of communication

Trust Model. Three entities, sender, receiver. Allow tampering on channel

Who is the adversary? Active adversary

Powers? Can change messages exchanged between sender and receiver

What constitutes a break? Change message without being detected

- orthogonal to secrecy, relevant regardless whether encryption is applied

One-Time Pad. example of perfect cipher

- $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^{\ell}$; Gen outputs a random ℓ-bit string k
- $\mathrm{Enc}_{\mathrm{k}}(\mathrm{m}) = \mathrm{k} \oplus \mathrm{m}$ (bit-wise XOR)

- attack: adversary flips the first bit; Q. what happens to message?
- error-detection codes are insufficent