DTTF/NB479: Dszquphsbqiz Day 12

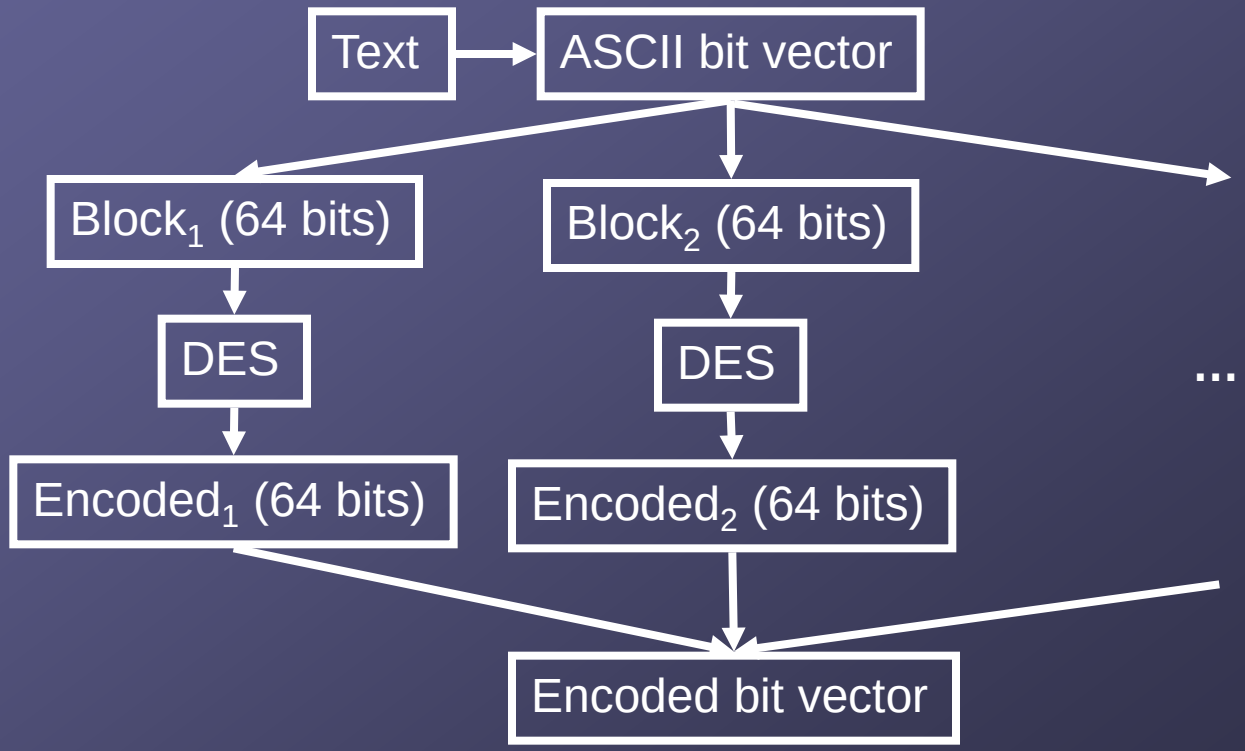
- Announcements:
  - Homework 2 returned
  - Monday: Written (concept and small calculations) exam on breaking ch 2 ciphers
  - HW 3 due date pushed back to Tuesday
- Next 2 weeks:
  - Data Encryption Standard (DES)
  - HW 4 (posted Monday, due 1.5 weeks later) is to implement DES
  - Rijndael, start RSA
- Questions?

The Chapter 2 Written Exam is next class

- Content:
  - Written problems
  - Concepts of the algorithms we discussed, how they work, how you can break them using various attacks
  - Inverses of integers and matrices (mod n)
  - Working out some examples by hand, like 5^{-1} mod (7)
  - Anything else from ch 1-2, but nothing that will require a computer.
- Rules:
  - Closed book and computer
  - You may bring a sheet with letters←→numbers, and inverses mod 26.
  - A scientific calculator is allowed

DES is a block cipher

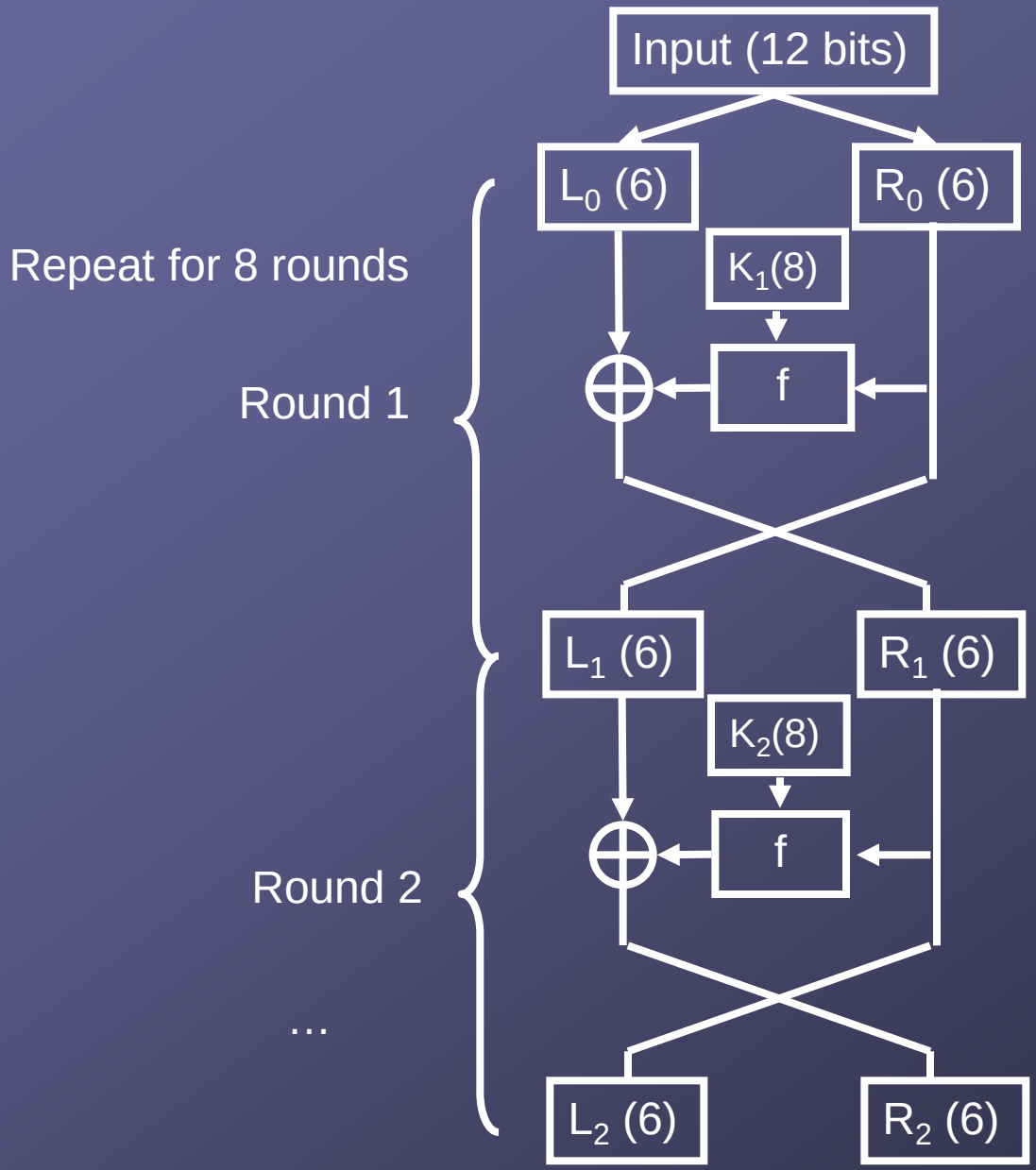
- History?
- Full-scale version operates on 64-bit blocks



EDEN is a toy version of DES that operates on 12-bit blocks

- EDEN is a term I coined:
  - ***E**asy*
  - ***D**ata*
  - ***E**ncryption*
  - ***N**on-standard*

EDEN



The key, K_i for round i is derived from a 9-bit key K.

1. Write L_1, R_1
2. We can decrypt by switching L and R and using the same procedure! (We need only to reverse the key sequence.) Example.

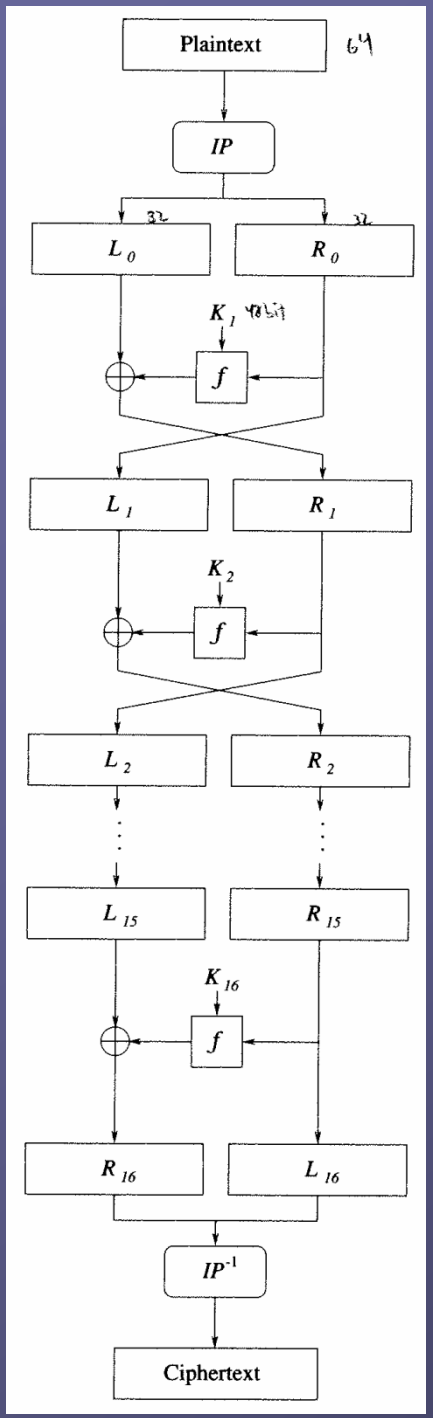
This is a *Feistel* system.

EDEN's encryption function f has the same three types of components as DES' f

1. Expanders
2. XOR with key
3. S-boxes

Read p. 116 to help with Q1-4.

Could you implement this?



DES has the same structure as EDEN except it uses initial permutations (IP)

Trappe &Washington, p. 125

The initial permutation table tells at which position in the input to find the output bit

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

<u>Reading permutation tables</u>

Say y = IP(x)

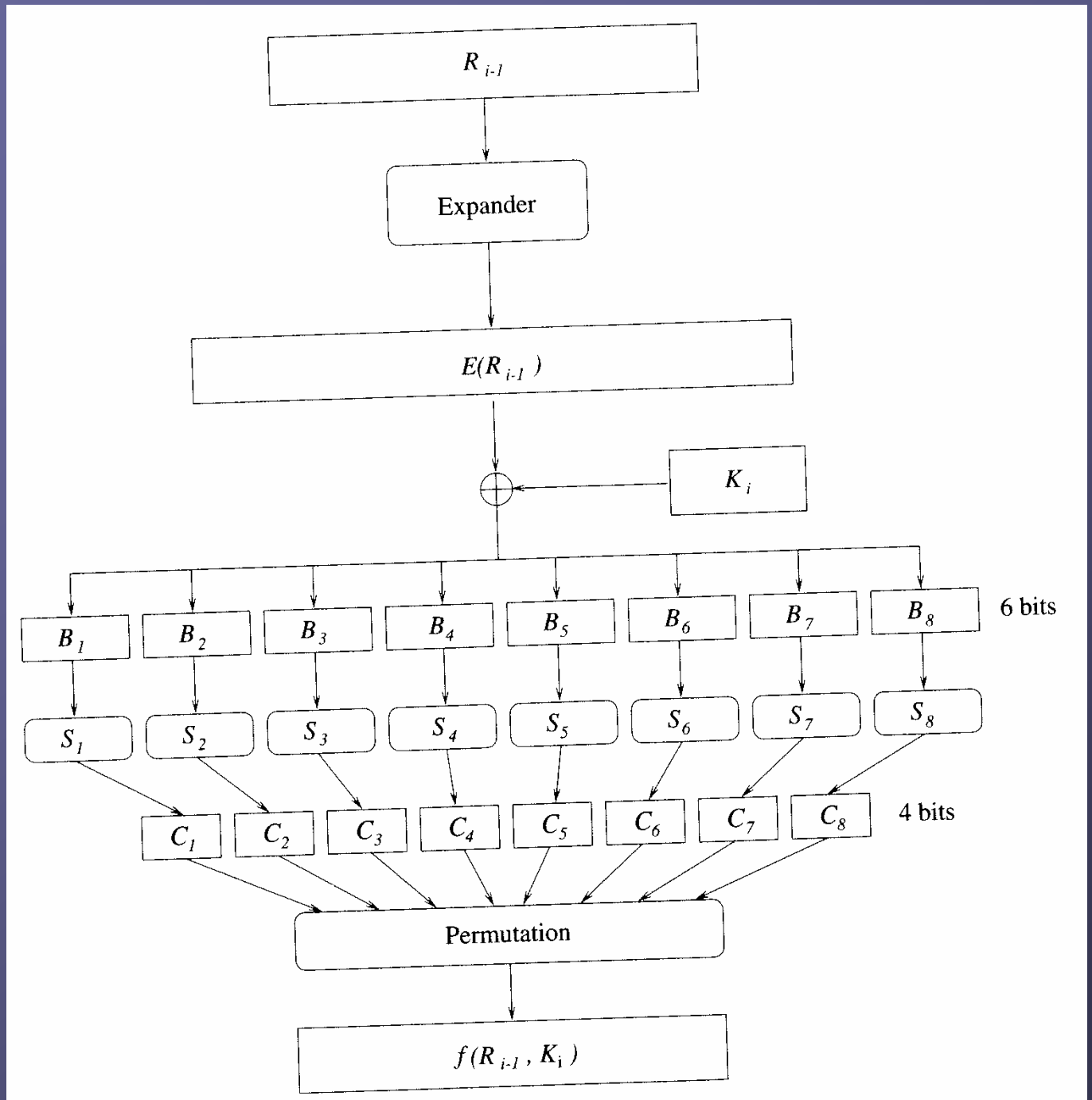
Then y[1] = x[58], y[2] = x[50], …

If $y = IP^{-1}(x)$,

y[58] = x[1], y[50] = x[2], …

Differences between DES & EDEN

EDEN	DES
12-bit blocks	64-bit blocks
	Extra initial permutation IP (for efficiency in 1970's?)
8 rounds	16 rounds
E: 6→8 bits	E: 32→48 bits
9 bit key: use 8/round	64-bit key: use 56/round Also contains extra permutations, a left-shift each round, and a reduction to 48 bits each round
2 S-boxes: 4→3 bits each	8 S-boxes: 6→4 bits each
	f ends by permuting the 32 bits


R_{i-1}
Expander
$E(R_{i-1})$
K_i
B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8
6 bits
S_1 S_2 S_3 S_4 S_5 S_6 S_7 S_8
C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8
4 bits
Permutation
$f(R_{i-1}, K_i)$

T&W, p. 126

DES round keys involve two permutations and a left shift

K =

0	1	1	1	1	1	1	0	0	1	0	0	1	0	0	0
1	1	0	0	0	0	1	0	1	0	0	0	0	0	1	0
0	0	0	1	1	1	0	0	0	0	0	0	1	1	1	0
1	1	1	1	0	1	0	0	1	1	1	0	1	0	0	0

Grab 56 permuted bits:[**57**, **49**, **41**, **33** …]

Get **1100**…

In round 1, LS(1), so: **100** …**1**

Then grab 48 permuted bits:

[14, 17, 11, 24, 1, 5, 3, …]

Get … **1** **0** …

T&W, p. 127