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
    - "Stuff You Don't Learn In School" workshop next Saturday – register by Wednesday to get free food.
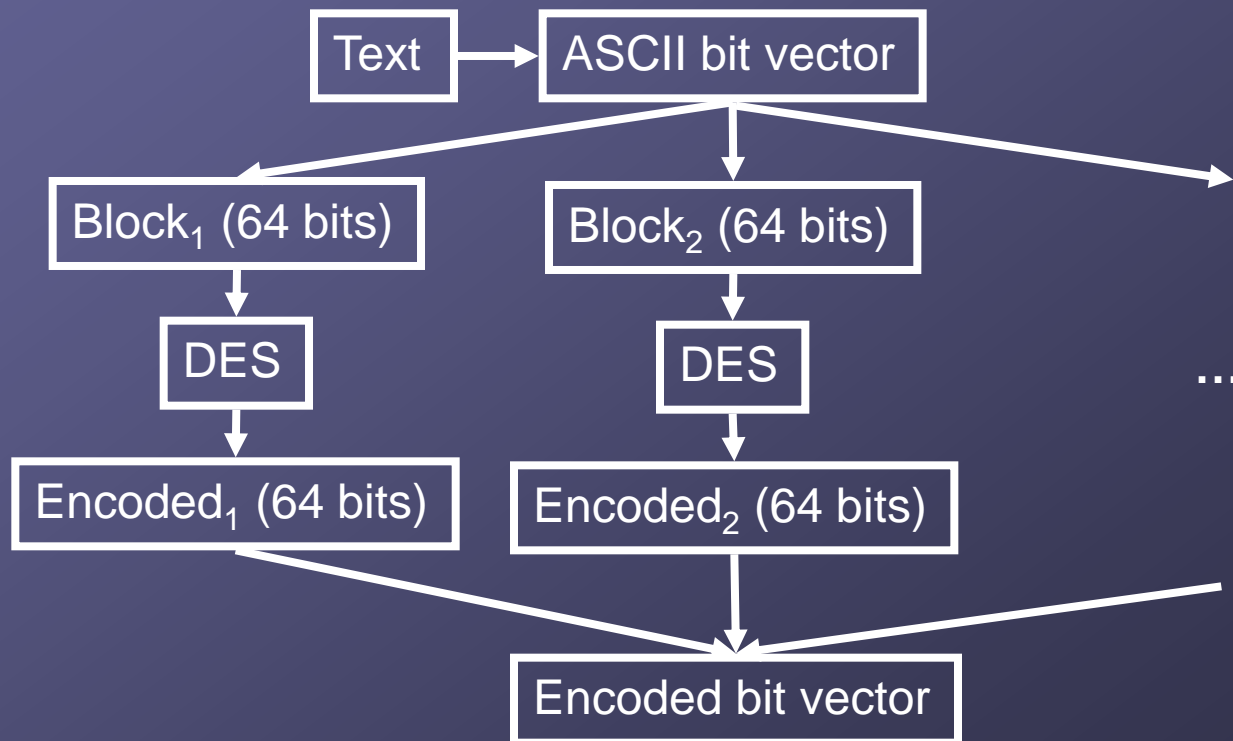
- Next 2 weeks:
    - Data Encryption Standard (DES)
    - HW 4 (posted Monday, due 1.5 weeks later) is to implement DES
    - Rijndael, start RSA

- Questions?

DES is a block cipher

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

```
        Text ───▶ ASCII bit vector
                         │
        ┌────────────────┼────────────────────────▶
        ▼                ▼
  Block₁ (64 bits)   Block₂ (64 bits)
        │                │
        ▼                ▼
      DES              DES                        ...
        │                │
        ▼                ▼
 Encoded₁ (64 bits)  Encoded₂ (64 bits)
        │                │
        └────────────────┼──────────────────
                         ▼
                 Encoded bit vector
```

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

Input (12 bits)

L_0 (6) R_0 (6)

Repeat for 8 rounds

$K_1(8)$

Round 1

⊕ ← f ←

L_1 (6) R_1 (6)

$K_2(8)$

⊕ ← f ←

Round 2

…

L_2 (6) R_2 (6)
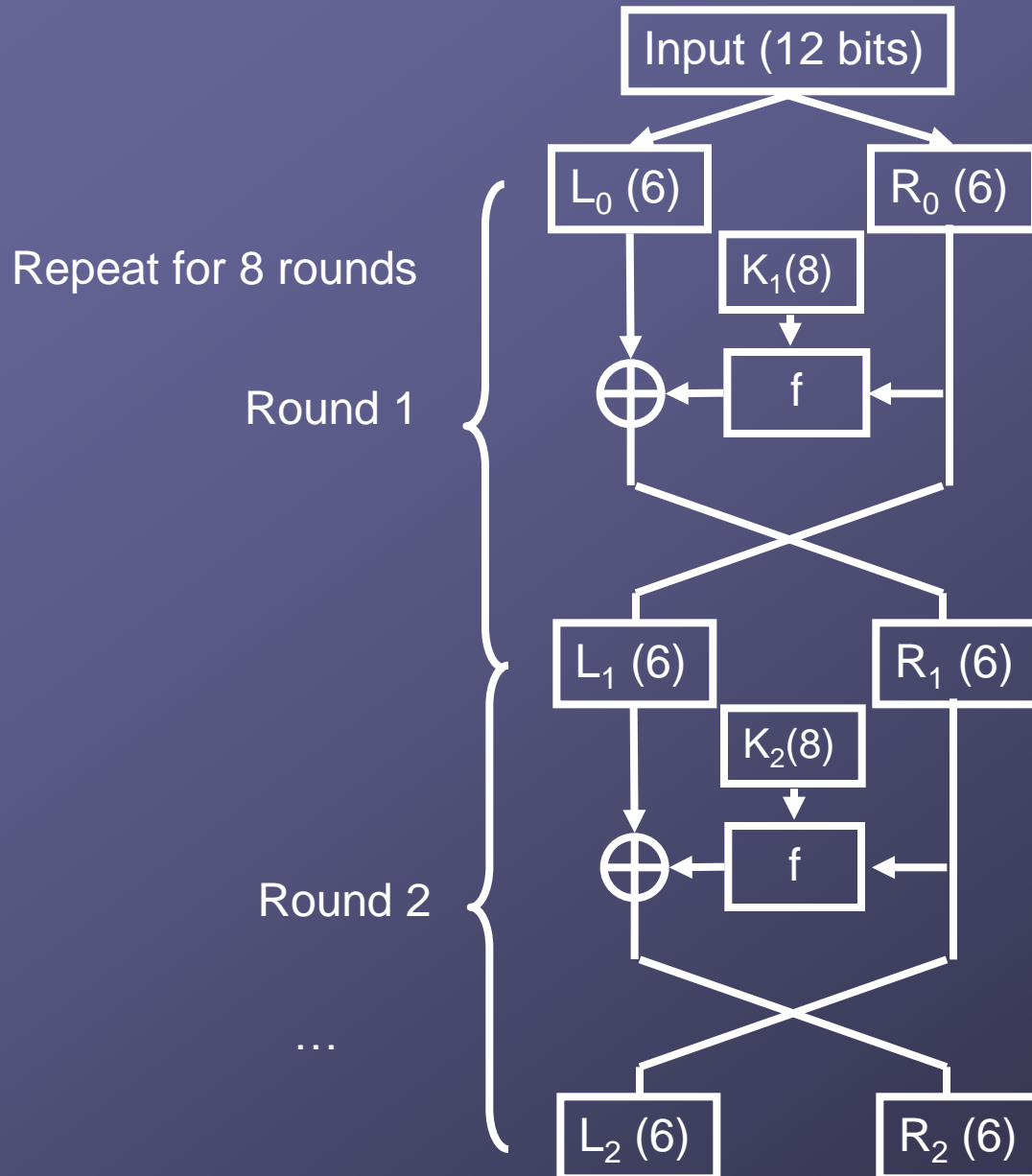
The key, K_i for round i is derived from a 9-bit key K.

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.
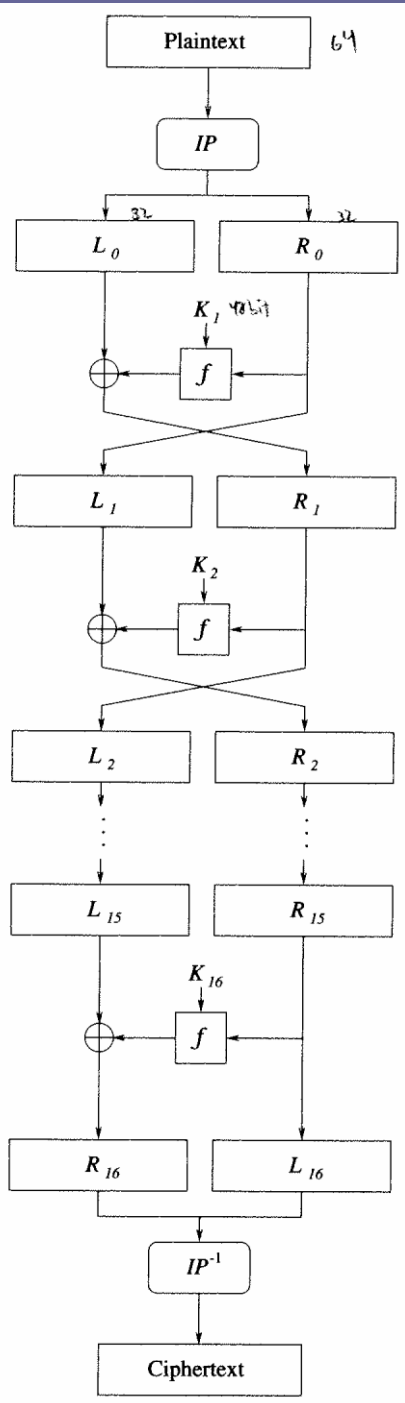
This is a *Feistel* system.

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)

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

Reading permutation tables
Say y = IP(x)
Then y[1] = x[58], y[2] = x[50], …

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