Lecture Notes

Advanced Discrete Structures

COT 4115.001 S15

2015-02-12

Recap

- Simplified DES-like Algorithm
- Modular Exponentiation

The Data Encryption Standard - Section 4.4

DES

The DES Algorithm

- Cipher blocks are 64-bits

- Key is 56-bits
  - Expressed as a 64-bit string
    - 8^{th}, 16^{th}, 24^{th}, bits used for parity checks
    - Each byte has an odd number of 1's

The DES Algorithm

- Algorithm has 3 stages

1. Bits in the message m are permuted by a fixed initial permutation (IP) to get

$$m_0 = IP(m) = L_0 R_0$$

(Here m and m_0 are 64-bit, and L_0 and R_0 are 32-bit.)

2. For $1 \leq i \leq 16$, perform the following

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

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

where K_i is a 48-bit string obtained from K

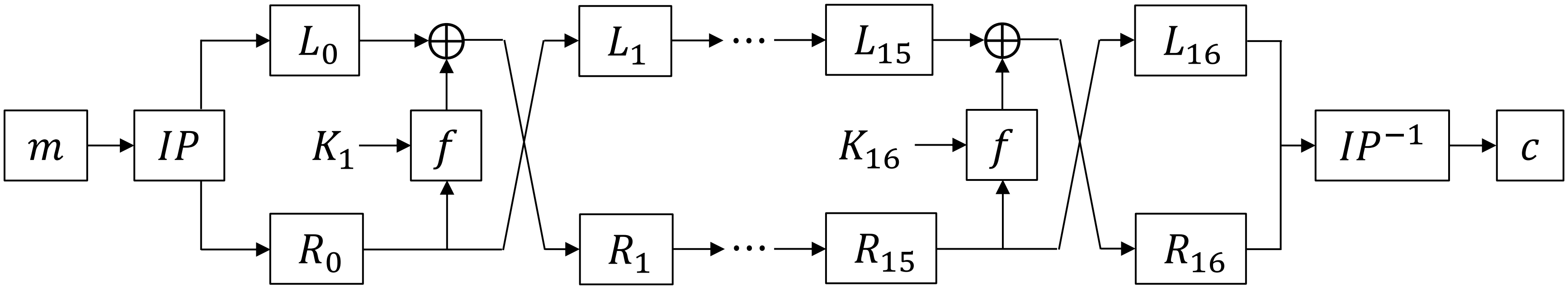
3. Switch left and right block to obtain $R_{16} L_{16}$, then apply the inverse of the initial permutation to get the ciphertext

$$c = IP^{-1}(R_{16} L_{16})$$

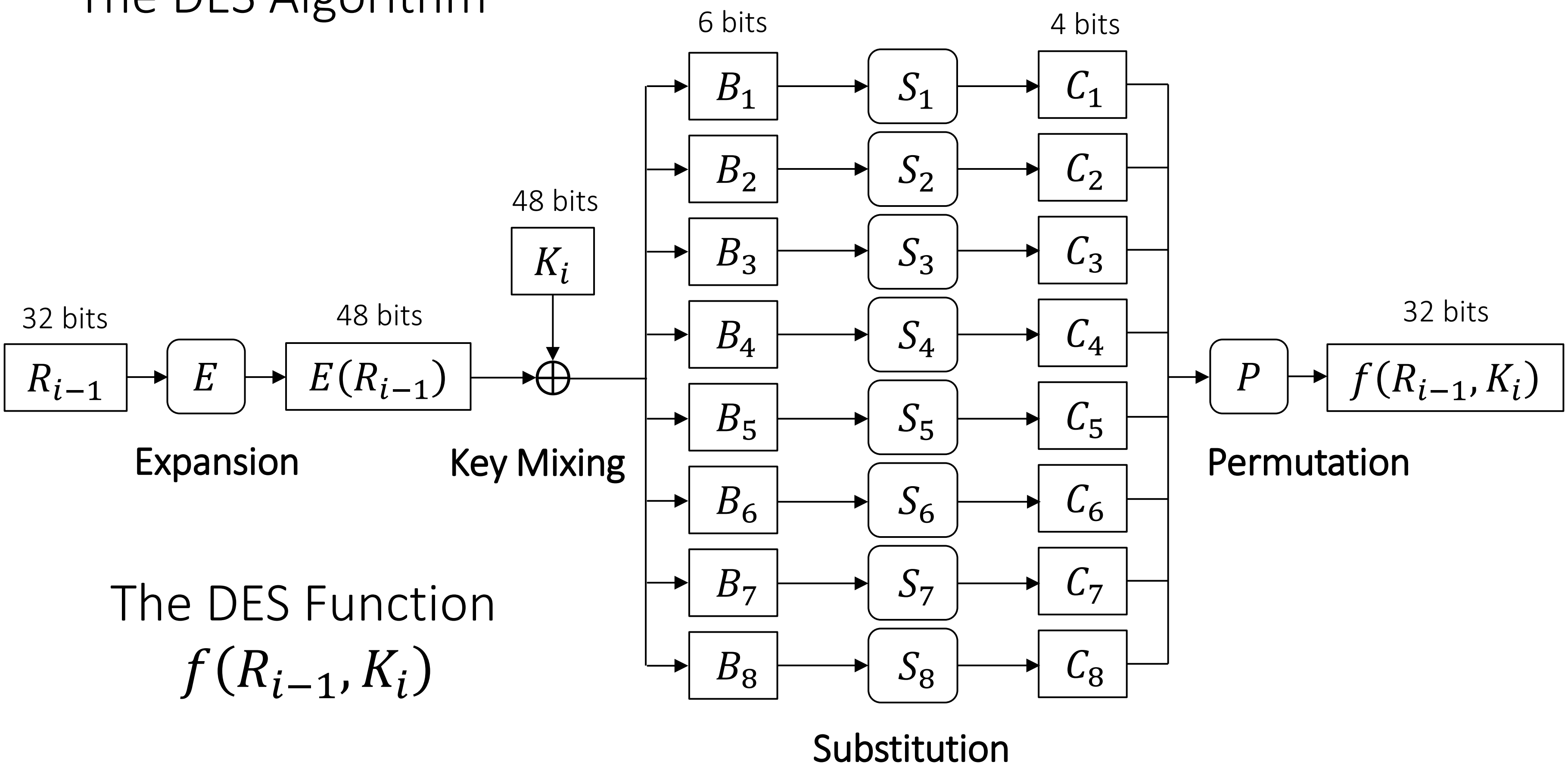
Encryption / Decryption

- <u>Encryption</u>: use keys $K_1, K_2, \ldots, K_n$

- <u>Decryption</u>: use keys $K_n, K_{n-1}, \ldots, K_1$



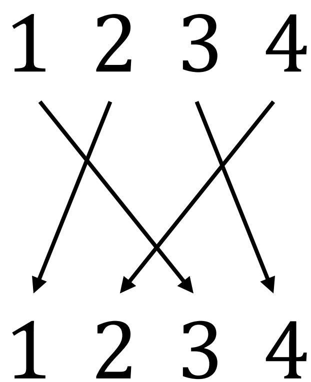
The DES Algorithm



The DES Function
$f(R_{i-1}, K_i)$

Permutations

- A *permutation* σ is a 1-1 and onto function from a set S to itself
- <u>Notations</u>: All express the same permutation



$$\begin{array}{l} 1 \rightarrow 3 \\ 2 \rightarrow 1 \\ 3 \rightarrow 4 \\ 4 \rightarrow 2 \end{array}$$

$$\boxed{\begin{array}{cc} 2 & 4 \\ 1 & 3 \end{array}}$$

Cauchy: $(3\ 1\ 4\ 2)$

Cyclic: $(1\ 3\ 4\ 2)$

DES – Initial Permutation (IP)

$$IP: \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64}$$

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

DES – Expansion Function (E)

$$E: \mathbb{Z}_2^{32} \to \mathbb{Z}_2^{48}$$

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

Example: 1110 0000 0101 1110 0000 1000 1011 1001

1111 0000 0000 0010 1111 1100 0000 0101 0001 0101 1111 0011

DES – S-Boxes

Example:

S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
100000	111101	010010	100000	000111	010001	111011	101000
0100	1110	1101	1010	1100	0110	0010	1001

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

DES – S-boxes

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	6	10	4	5	3

DES – S-boxes

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\boldsymbol{S}_6$	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
$\boldsymbol{S}_7$	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
$\boldsymbol{S}_8$	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

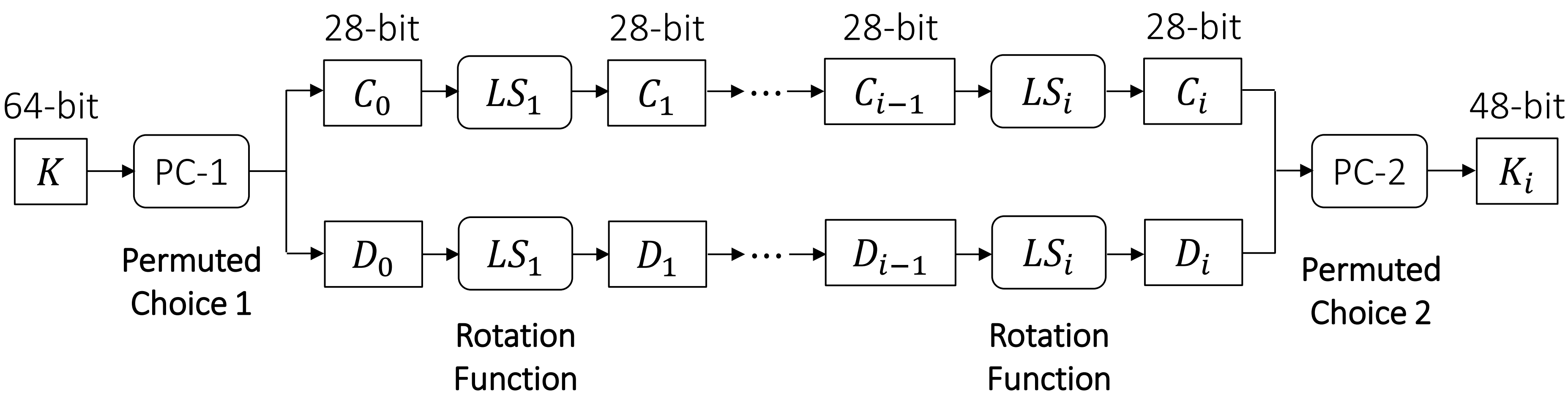
DES – Permutation (P)

$$P: \mathbb{Z}_2^{32} \rightarrow \mathbb{Z}_2^{32}$$

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

DES – Round Key K_i Generation

1. Permuted Choice 1 (PC-1)
2. Rotation Function (LS_i)
3. Permuted Choice 2 (PC-2)



DES – Permuted Choice 1 (PC_1)

- K is 64 bits, but only 56 are used (no $8, 16, 24, 32, 40, 48, 56$)

  1. Discard parity bits and permute key simultaneously with the Key Permutation:

$$PC_1 \colon \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{56}$$

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

DES – Rotation Function (LS_i)

2. Split the result of the Key Permutation into two 28-bit blocks:

$$KP(K) = C_0 D_0$$

For $1 \leq i \leq 16$, let

$$C_i = LS_i(C_{i-1}) \qquad \text{and} \qquad D_i = LS_i(D_{i-1})$$

where LS_i means shifting bits to the left by 1 or 2, according to the following schedule:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
LS_i shift	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

<u>Example</u>:

$$C_0 = 0000\ 1110\ 1101\ 1000\ 1101\ 0000\ 111\underline{0}$$

$$C_1 = 0001\ 1101\ 1011\ 0001\ 1010\ 0001\ 11\underline{0}0$$

$$C_2 = 0011\ 1011\ 0110\ 0011\ 0100\ 0011\ 1\underline{0}00$$

$$C_3 = 1110\ 1101\ 1000\ 1101\ 0000\ 111\underline{0}\ 0000$$

DES – Wrap-up

- Permutations IP and IP^{-1} serve *no cryptographic purpose*
  - Facilitate loading blocks in and out of mid-1970s 8-bit based hardware
- Design of the S-Boxes a mystery until IBM published their criteria
  1. Each S-Box has 6 inputs and 4 output bits (largest to fit on a chip in 1974)
  2. Outputs of S-Boxes should not be close to a linear function
  3. Each row of an S-Box must contain all numbers 0 to 15
  4. If two inputs of an S-Box differ by 1 bit, the outputs differ by at least 2 bits
  5. If two inputs differ in the first 2 bits, but have the same last 2 bits, the outputs must be unequal
  6. There are 32 pairs of inputs having a given XOR. For each pair of these pairs, compute the XORs of the outputs. No more than 8 of these output XORs should be the same. (To avoid differential cryptanalysis)
  7. Something similar to (6), but for combinations of three S-boxes.

DES – Permuted Choice 2 (PC_2)

3. 48 bits out of the 56-bit string $C_i D_i$ are chosen to be K_i

$$PC_2 : \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{56}$$

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

(9, 18, 22, 25, 35, 38, 43, 54 are missing)

The Data Encryption Standard - Section 4.4.1

DES IS NOT A GROUP

Double Encryption?

- A potential way to increase the key size is to double encrypt
  - Choose keys K_1 and K_2 and encrypt the plaintext P by $E_{K_2}\left(E_{K_1}(P)\right)$
  - In some cipher systems, $E_{K_2}\left(E_{K_1}(P)\right) = E_{K_3}(P)$ for some key K_3
    - Affine ciphers, RSA
- The question, “Is DES a group?” is asking “For each E_{K_1} and E_{K_2}, does there exists a $E_{K_3} = E_{K_2}\,E_{K_1}$?”
  - Restated, “Is encryption closed under composition?”

DES is not a group (Sketch)

- Let E_0 and E_1 represent encryption with the keys $K = 000 \ldots 00$ and $K = 111 \ldots 11$, respectively
- Repeatedly apply $E_1 \circ E_0$ to certain plaintext yielded the original message after 2^{32} iterations
- A sequence of encryptions (for some plaintext P),

$$E_1 E_0(P), E_1 E_0(E_1 E_0(P)), (E_1 E_0)^3(P), \ldots, (E_1 E_0)^n(P) = P$$

where n is the smallest positive integer such that $(E_1 E_0)^n(P) = P$ is called a *cycle* of length n.

Lemma. If m is the smallest positive integer such that

$$(E_1E_0)^m(P) = P,$$

and n is the length of a cycle, then $n \mid m$.

Proof. Let n be the length of the cycle corresponding to

$$(E_1E_0)^n(P_0) = P_0 \,.$$

Since m is taken as the greatest cycle length, $m \geq n$. By the division algorithm, there exist $q \in \mathbb{Z}$ and $0 \leq r < n$ such that $m = q\,n + r$ **.** This means

$$P_0 = (E_1E_0)^m(P_0) = (E_1E_0)^r(E_1E_0)^{qn}(P_0) = (E_1E_0)^r(P_0),$$

but $r < n$ which contradicts that n is the cycle length unless $r = 0$. In that case, $n \mid m$. ■

DES is not a group (Sketch)

- Suppose DES is closed under composition
  - $E_1 E_0 = E_K$ for some key K
  - ${E_K}^2 = E_K E_K = E_L$ for some key L,
    - Similar for ${E_K}^3, {E_K}^4, \ldots$
- There are only 2^{56} keys, so $m \leq 2^{56}$ for m in lemma
- 33 different cycles were exhibited for a particular plaintext P_0 so each of their lengths must divide m
  - The smallest m that could satisfy this is around 10^{277} which contradicts that $m \leq 2^{56}$
  - DES is not closed under composition, i.e., not a group!