Dr. A. Betten Fall 2006

M360 Mathematics of Information Security

homework sheet # 4

Problem # 1

Check whether the following arguments are logical or not. Explain!

a) i) If Alice is wrong, then Bill is wrong. If Bill is wrong, then Connie is wrong. Connie is wrong. Therefore, Alice is wrong.

ii) If turtles can sing, then artichokes can fly. If artichokes can fly, then turtles can sing and dogs can't play chess. Dogs can play chess if and only if turtles can sing. Therefore, turtles can't sing.

iii) If I oversleep, I will miss the bus. If I miss the bus, I'll be late for work unless Sue gives me a ride. If Sue's car is not working, she won't give me a ride. If I am late for work, I'll lose my job unless the boss is away. Sue's car is not working. The boss is not away. Therefore, if I oversleep, I'll lose my job.

b) And a selection from Lewis Carroll:

i) No ducks waltz. No officers ever decline to waltz. All my poultry are ducks. Therefore, my poultry are not officers.

ii) Everyone who is sane can do Logic. No lunatics are fit to serve on a jury. None of your sons can do Logic. Therefore, none of your sons are fit to serve on a jury.

iii) The only articles of food, that my doctor allows me, are such as are not very rich. Nothing that agrees with me is unsuitable for supper. Wedding-cake is always very rich. My doctor allows me all articles of food that are suitable for supper. Therefore, wedding-cake always disagrees with me.

iv) Animals, that do not kick, are always unexcitable. Donkeys have no horns. A buffalo can always toss one over a gate. No animals that kick are easy to swallow. No hornless animal can toss one over a gate. All animals are excitable, except buffaloes. Therefore, donkeys are not easy to swallow.

Problem # 2

Decrypt the simple-DES ciphertext

AQMn

using the key 011010011. Use the table below to code symbols to 6-bit integers. Use the simple-DES machines on the attached sheets (note that you have to change something for decryption). The S-boxes are:

$$S_1 : \begin{bmatrix} 101 & 010 & 001 & 110 & 011 & 100 & 111 & 000 \\ 001 & 100 & 110 & 010 & 000 & 111 & 101 & 011 \end{bmatrix}$$

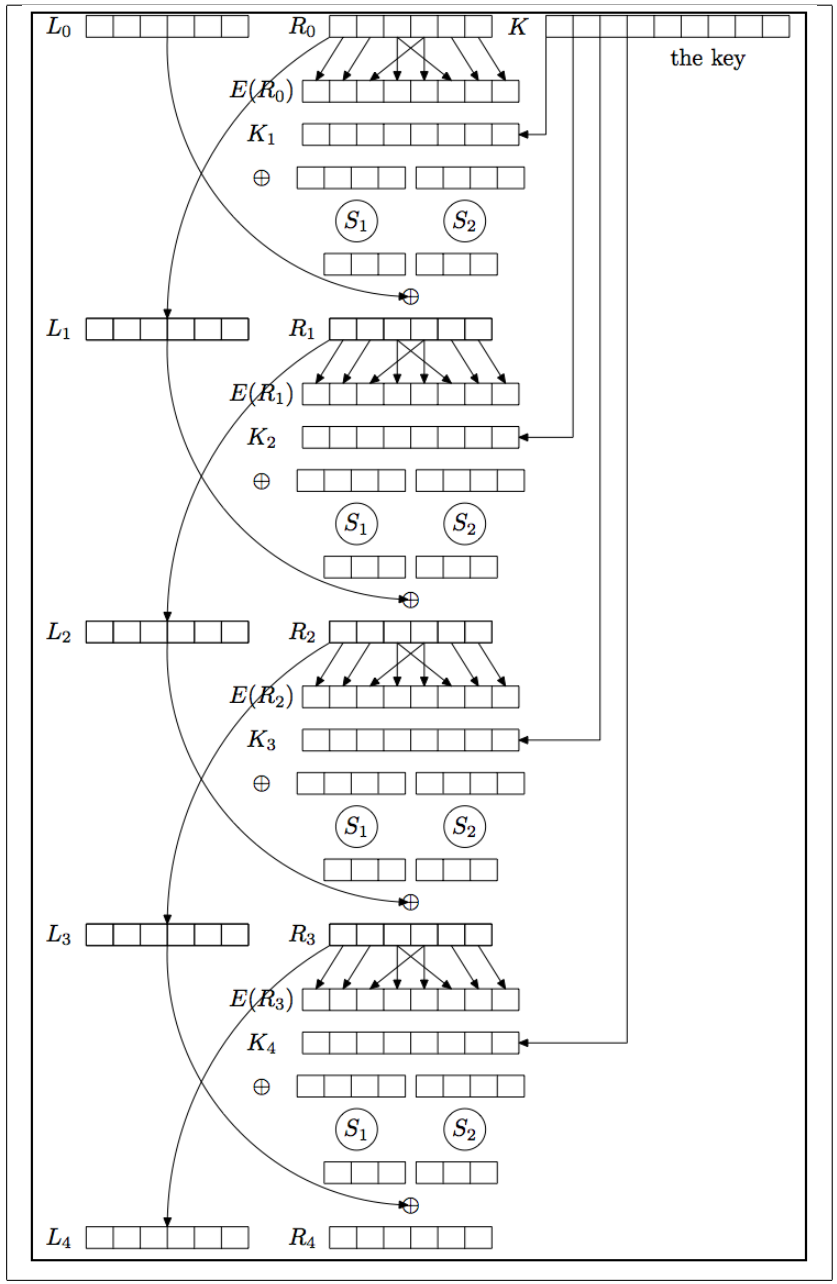
$$S_2 : \begin{bmatrix} 100 & 000 & 110 & 101 & 111 & 001 & 011 & 010 \\ 101 & 011 & 000 & 111 & 110 & 010 & 001 & 100 \end{bmatrix}$$

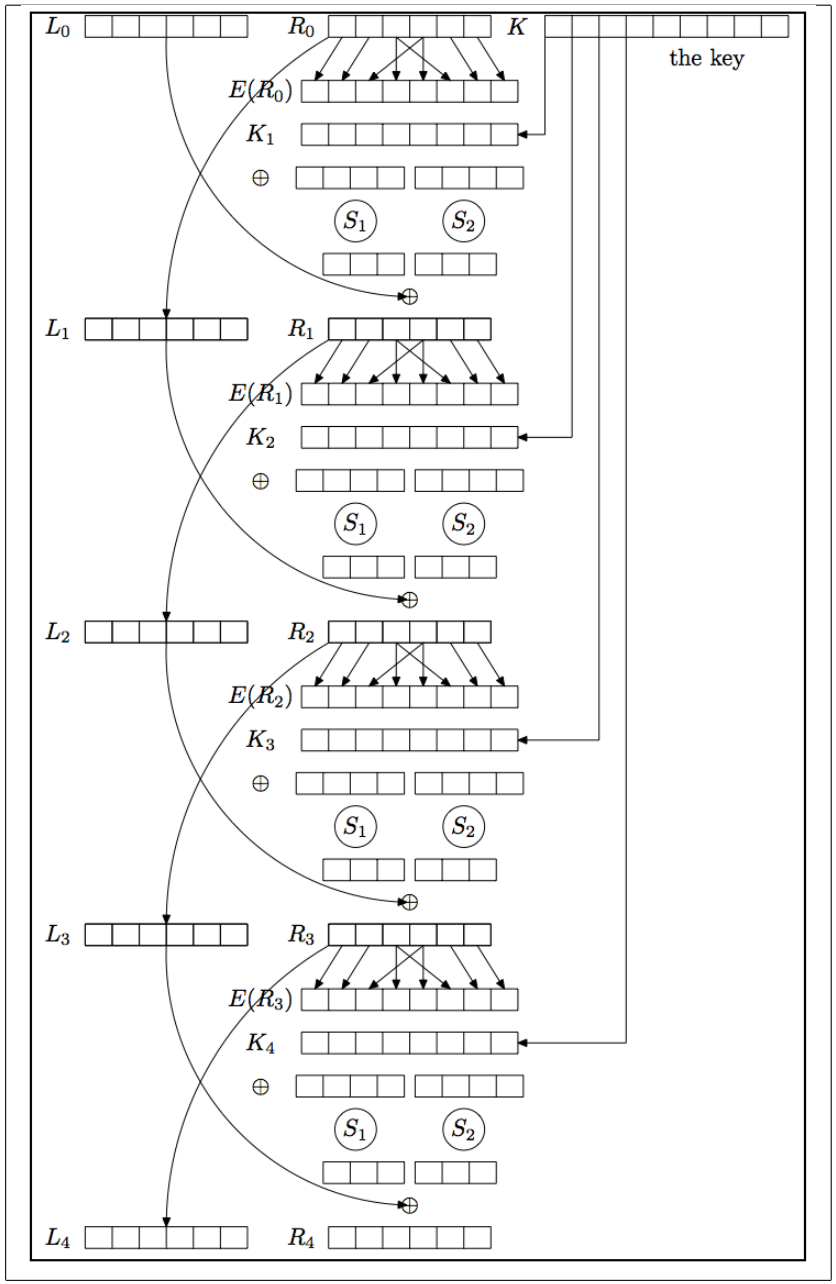
	dec.	binary
a	0	000000
b	1	000001
c	2	000010
d	3	000011
e	4	000100
f	5	000101
g	6	000110
h	7	000111
i	8	001000
j	9	001001
k	10	001010
l	11	001011
m	12	001100
n	13	001101
o	14	001110
p	15	001111

	dec.	binary
q	16	010000
r	17	010001
s	18	010010
t	19	010011
u	20	010100
v	21	010101
w	22	010110
x	23	010111
y	24	011000
z	25	011001
' '	26	011010
0	27	011011
1	28	011100
2	29	011101
3	30	011110
4	31	011111

	dec.	binary
A	32	100000
B	33	100001
C	34	100010
D	35	100011
E	36	100100
F	37	100101
G	38	100110
H	39	100111
I	40	101000
J	41	101001
K	42	101010
L	43	101011
M	44	101100
N	45	101101
O	46	101110
P	47	101111

	dec.	binary
Q	48	110000
R	49	110001
S	50	110010
T	51	110011
U	52	110100
V	53	110101
W	54	110110
X	55	110111
Y	56	111000
Z	57	111001
'.'	58	111010
5	59	111011
6	60	111100
7	61	111101
8	62	111110
9	63	111111


L_0
R_0
K
the key
$E(R_0)$
K_1
$\oplus$
S_1
S_2
L_1
R_1
$E(R_1)$
K_2
$\oplus$
S_1
S_2
L_2
R_2
$E(R_2)$
K_3
$\oplus$
S_1
S_2
L_3
R_3
$E(R_3)$
K_4
$\oplus$
S_1
S_2
L_4
R_4


L_0
R_0
K
the key
$E(R_0)$
K_1
$\oplus$
S_1
S_2
L_1
R_1
$E(R_1)$
K_2
$\oplus$
S_1
S_2
L_2
R_2
$E(R_2)$
K_3
$\oplus$
S_1
S_2
L_3
R_3
$E(R_3)$
K_4
$\oplus$
S_1
S_2
L_4
R_4