

Exercice 2

PARTIE A

- 1b
- 2c
- 3b
- 4d

PARTIE B

1

P3	P3	P2	P1	P1	P1	P2	P2	P3	P3	
0	1	2	3	4	5	6	7	8	9	10

2

Il s'agit du scénario 2 car nous nous retrouvons dans la situation où P1 possède R1 et attend R2 avant de pouvoir continuer et P3 possède R2 et attend R1 avant de pouvoir continuer.

PARTIE C

1a

0100 0110 => 46 en hexa => caractère F 0110 0011 => 63
en hexa => caractère c donc cF

1b

0b 1000 1101 1011 0110

2a

a	b	(a xor b) xor b
0	0	0
0	1	0
1	0	1
1	1	1

2b

On peut remarquer que $(a \text{ xor } b) \text{ xor } b$ permet de retrouver a, donc si a correspond au message non chiffré et $a \text{ xor } b$ correspond au message chiffré, un $(a \text{ xor } b) \text{ xor } b$ permet donc de retrouver le message non chiffré. Si on appelle m le message non chiffré, m' le message chiffré et k la clé de chiffrement, un $m' \text{ xor } k$ permettra de retrouver m.