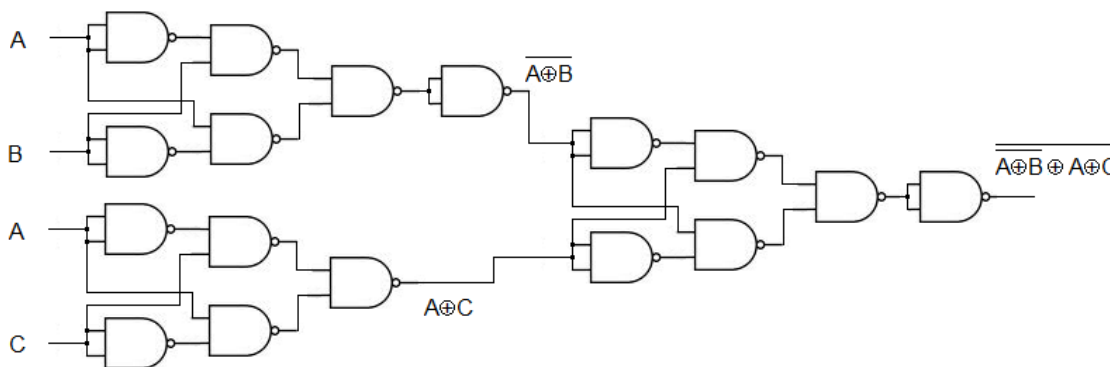


A seguir substitui-se cada uma das portas pela sua equivalente NAND:



2- Um sistema comum de encriptação, encontrado em muitos protocolos de comunicação em redes de computadores, designa-se por “one time pad”. Admita-se que um computador A quer enviar uma mensagem  $m$  para um segundo computador B. Imagine-se que essa mensagem é composta por uma sequência de  $n$  bits. Considere-se ainda que ambos os computadores concordam com uma palavra-chave  $k$  utilizada para encriptar e desencriptar a mensagem. A palavra-chave possui o mesmo número de bits da mensagem. A mensagem codificada  $c$  que o computador A envia para o computador B é obtida pela operação Ou-Exclusivo entre a mensagem  $m$  e a palavra-chave  $k$ . O computador B desencripta a mensagem recebida  $c$  efectuando a mesma operação lógica com a mesma palavra-chave  $k$ .

a) Imagine que, em hexadecimal,  $m=4AF0_{16}$  e  $k=ABCD_{16}$ . Indique, também em hexadecimal, a mensagem codificada  $c$ . [3]

Primeiro converte-se  $m$  e  $k$  para binário:

$$m = 0100.1010.1111.0000$$

$$k = 1010.1011.1100.1101$$

Segundo executa-se a operação OU-Exclusivo entre  $m$  e  $k$ :

$$c = 1110000100111101$$

Terceiro converte-se o resultado para hexadecimal:

$$c = E13D_{16}$$

b) Mostre que  $m$  pode ser obtido através da operação XOR entre  $c$  e  $k$ . [1]

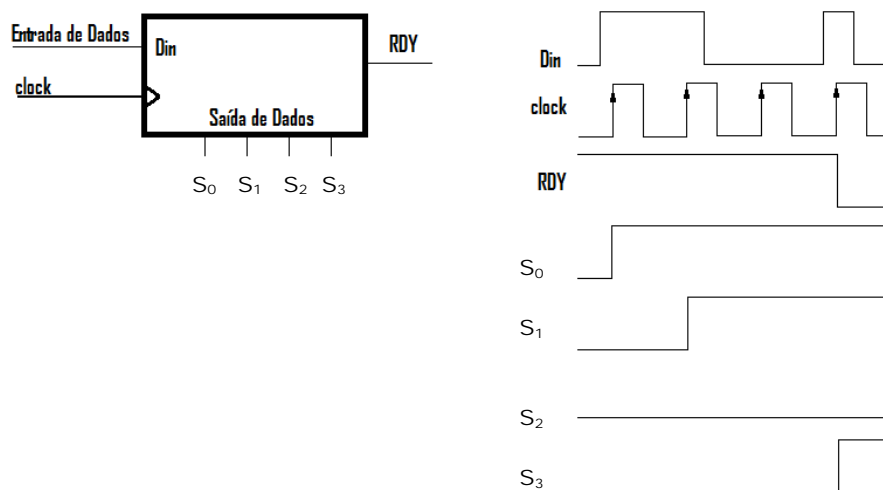


Para resolver esta alínea basta iterar uma única vez a tabela de transição de estados tendo em consideração que o estado presente é  $Q=000$ . Assim,

Estado Presente			Estado Seguinte			Entradas de clear e preset					
$Q_2$	$Q_1$	$Q_0$	$Q_2$	$Q_1$	$Q_0$	$\overline{P_2}$	$\overline{C_2}$	$\overline{P_1}$	$\overline{C_1}$	$\overline{P_0}$	$\overline{C_0}$
0	0	0	0	0	1	1	1	1	1	1	1

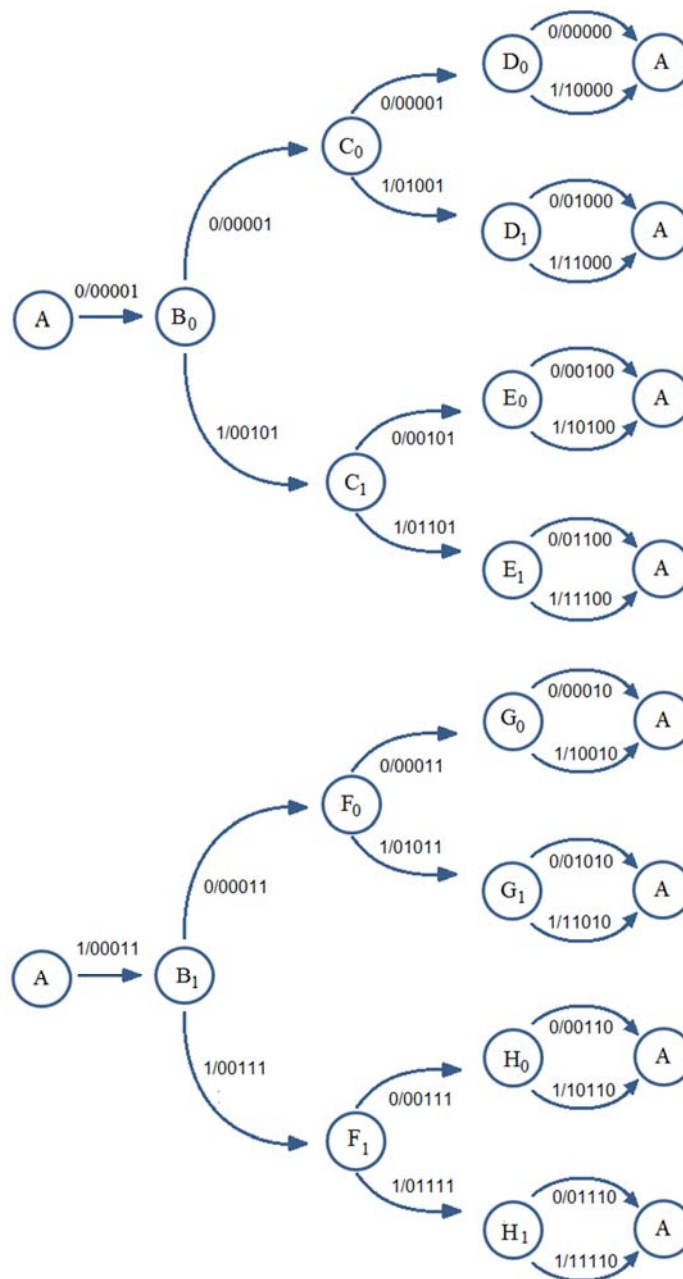
Logo o estado seguinte a 000 é 001.

**4- Conversor Série-Paralelo.** Projecte um circuito digital sequencial com **flip-flop's tipo D** capaz de converter uma palavra de 4 bits, recebidos no formato série, para o formato paralelo. O circuito deve possuir **uma entrada de dados e uma entrada de clock** e deve possuir **5 saídas**: 4 para os bits de dados e uma adicional, que se designa por **RDY**, que indica que a palavra à saída se encontra pronta para ser lida. Essa indicação consiste numa transição descendente do sinal **RDY**. O desenho que se segue ilustra o processo. [4]



R: Começamos por representar a máquina de estados associada ao problema. Neste caso optou-se por um modelo de Mealy onde as transições têm o formato  $D_{in}/ S_3 S_2 S_1 S_0 RDY$ . A máquina tem o seguinte aspecto:

(Nota: Para facilitar a legibilidade a máquina de estados encontra-se dividida em duas partes)



Existem, ao todo, 15 estados. Logo vão ser necessários 4 flip-flop's (neste caso tipo D). Em seguida efectua-se a atribuição de estados.

A	B0	B1	C0	C1	D0	D1	E0	E1	F0	F1	G0	G1	H0	H1
0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110

Passamos agora à tabela de transição de estados:

Estado Presente		Entrada D <sub>in</sub>	Estado Seguente	Flip-Flop	Saídas		
				D <sub>3</sub> D <sub>2</sub> D <sub>1</sub> D <sub>0</sub>	S <sub>3</sub> S <sub>2</sub> S <sub>1</sub> S <sub>0</sub>	RDY	
A	0000	0	0001	0001	0000	1	
A	0000	1	0010	0010	0001	1	
B0	0001	0	0011	0011	0000	1	
B0	0001	1	0100	0100	0010	1	
B1	0010	0	1001	1001	0000	1	
B1	0010	1	1010	1010	0100	1	
C0	0011	0	0101	0101	0010	1	
C0	0011	1	0110	0110	0110	1	

C1	0100	0	0111	0111	0000	0
C1	0100	1	1000	1000	1000	0
D0	0101	0	0000	0000	0100	0
D0	0101	1	0000	0000	1100	0
D1	0110	0	0000	0000	0010	0
D1	0110	1	0000	0000	1010	0
E0	0111	0	0000	0000	0110	0
E0	0111	1	0000	0000	1110	0
E1	1000	0	0000	0000	0001	1
E1	1000	1	0000	0000	0011	1
F0	1001	0	1011	1011	0001	1
F0	1001	1	1100	1100	0101	1
F1	1010	0	1101	1101	0011	1
F1	1010	1	1110	1110	0111	1
G0	1011	0	0000	0000	0001	0
G0	1011	1	0000	0000	1001	0
G1	1100	0	0000	0000	0101	0
G1	1100	1	0000	0000	1101	0
H0	1101	0	0000	0000	0011	0
H0	1101	1	0000	0000	1011	0
H1	1110	0	0000	0000	0111	0
H1	1110	1	0000	0000	1111	0

Recorrendo aos mapas de Karnaugh, e considerando irrelevante as saídas para o estado 1111, obtêm-se as seguintes equações de excitação:

$$D_3 = \overline{Q_2} \cdot \overline{Q_1} \cdot \overline{Q_0} + Q_3 \cdot \overline{Q_2} \cdot \overline{Q_1} \cdot Q_0 + \overline{Q_3} \cdot Q_2 \cdot \overline{Q_1} \cdot \overline{Q_0} \cdot D_{in}$$

$$D_2 = \overline{Q_3} \cdot \overline{Q_2} \cdot \overline{Q_1} \cdot Q_0 + Q_3 \cdot \overline{Q_2} \cdot \overline{Q_1} \cdot \overline{Q_0} + \overline{Q_2} \cdot \overline{Q_1} \cdot Q_0 \cdot D_{in} + \overline{Q_3} \cdot Q_2 \cdot \overline{Q_1} \cdot \overline{Q_0} \cdot D_{in}$$

$$D_1 = \overline{Q_3} \cdot \overline{Q_2} \cdot \overline{Q_1} \cdot D_{in} + \overline{Q_3} \cdot \overline{Q_2} \cdot \overline{Q_0} \cdot D_{in} + \overline{Q_2} \cdot \overline{Q_1} \cdot \overline{Q_0} \cdot D_{in} + \overline{Q_2} \cdot \overline{Q_1} \cdot Q_0 \cdot D_{in} + \overline{Q_3} \cdot Q_2 \cdot \overline{Q_1} \cdot \overline{Q_0} \cdot D_{in}$$

$$D_0 = \left( \overline{Q_3} \cdot \overline{Q_2} + \overline{Q_2} \cdot \overline{Q_1} \cdot Q_0 + \overline{Q_2} \cdot \overline{Q_1} \cdot \overline{Q_0} + \overline{Q_3} \cdot \overline{Q_1} \cdot \overline{Q_0} \right) \cdot D_{in}$$

$$S_3 = \overline{Q_2} \cdot D_{in} + Q_3 \cdot \overline{Q_1} \cdot Q_0 \cdot D_{in}$$

$$S_2 = \overline{Q_3} \cdot \overline{Q_2} \cdot Q_0 + Q_3 \cdot \overline{Q_2} \cdot \overline{Q_0} + \overline{Q_3} \cdot \overline{Q_2} \cdot \overline{Q_1} \cdot Q_0 \cdot D_{in} + \overline{Q_3} \cdot \overline{Q_2} \cdot \overline{Q_1} \cdot D_{in} + \overline{Q_2} \cdot \overline{Q_1} \cdot \overline{Q_0} \cdot D_{in}$$

$$S_1 = \overline{Q_2} \cdot \overline{Q_1} + \overline{Q_3} \cdot \overline{Q_2} \cdot Q_0 + \overline{Q_3} \cdot \overline{Q_1} \cdot Q_0 + \overline{Q_3} \cdot \overline{Q_1} \cdot \overline{Q_0} + \overline{Q_3} \cdot \overline{Q_2} \cdot Q_0 \cdot D_{in} + \overline{Q_3} \cdot \overline{Q_2} \cdot \overline{Q_0} \cdot D_{in}$$

$$S_0 = \overline{Q_3} + \overline{Q_2} \cdot \overline{Q_1} \cdot \overline{Q_0} \cdot D_{in}$$

$$RDY = \overline{Q_3} \cdot \overline{Q_2} \cdot \overline{Q_1} + \overline{Q_2} \cdot \overline{Q_1} \cdot Q_0 + \overline{Q_3} \cdot \overline{Q_2} \cdot \overline{Q_0} + \overline{Q_2} \cdot \overline{Q_0} \cdot D_{in}$$

(Nota: 80% da cotação desta questão é atribuída à máquina de estados, 15% à tabela de transição de estados e o restante às equações de excitação)