

---

**EXAMEN FINAL DE CRIPTOGRAFIA**  
**FACULTAT D'INFORMÀTICA DE BARCELONA (UPC)**  
**10 de juny de 2003**

---

1. Esquema i descripció breu del funcionament dels sistemes de xifrat en flux.
2. Quina d'aquestes dues taules correspon a una caixa S del DES? Per què? Per a aquesta caixa, quina és la sortida corresponent a l'entrada  $B = 011011$ ?

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

3. Funcionament del mode d'operació CBC.
4. Funcions unidireccionals: definició, ús criptogràfic, exemples.
5. Quins algoritmes de signatura digital admet l'estàndard DSS actualment vigent?  
Per a cadascun d'ells, com són els paràmetres del sistema i les claus, públiques i privades, d'un usuari?
6. Què és un certificat digital? Com s'utilitza?

**Puntuació:** Cada pregunta val **1 punt**